Tables of modular Galois representations

Nicolas Mascot

Tables of modular Galois representations

Nicolas Mascot*

University of Warwick, supported by EPSRC Programme Grant "LMF: L-Functions and Modular Forms". Formerly IMB, Université Bordeaux 1, UMR 5251, F-33400 Talence, France. CNRS, IMB, UMR 5251, F-33400 Talence, France. INRIA, project LFANT, F-33400 Talence, France.

December 17, 2014

Abstract

We give tables of modular Galois representations obtained using the algorithm which we described in [Mas13]. We computed Galois representations modulo primes up to 31 for the first time. In particular, we computed the representations attached to a newform with non-rational (but of course algebraic) coefficients, which had never been done before. These computations take place in the jacobian of modular curves of genus up to 26. We also show how these computation results can be partially proved.

Acknowledgements

I heartily thank my advisor J.-M. Couveignes for offering me to work on this beautiful subject. The computations presented here would not have been amenable without Bill Allombert, who suggested to me the idea of step-by-step polynomial reduction, and Karim Belabas and Denis Simon, who provided me their [BS14] script. I am therefore extremely grateful to them.

The computations presented in this paper were carried out using the PlaFRIM experimental testbed, being developed under the Inria PlaFRIM development action with support from LABRI and IMB and other entities: Conseil Régional d'Aquitaine, FeDER, Université de Bordeaux and CNRS (see https://plafrim.bordeaux.inria.fr/). The softwares used were [SAGE] and [Pari/GP].

This research was supported by the French ANR-12-BS01-0010-01 through the project PEACE, and by the DGA maîtrise de l'information.

*N.A.V.Mascot@Warwick.ac.uk

We begin with a short summary about Galois representations attached to modular forms and how we used these in [Mas13] to compute Fourier coefficients of modular forms in section 1. This computation becomes much easier if the polynomial in $\mathbb{Q}[X]$ defining the representation is reduced, and we show new ideas to do so efficiently in section 2. We then present tables of results of our computations in the last section 3. Finally, since these results rely on the identification of rational numbers given in approximate form, we present in section 4 a method to formally prove that the number field cut out by the Galois representation has been correctly computed.

1 Background summary

Let $f = q + \sum_{n=2}^{+\infty} a_n q^n \in S_k\big(\Gamma_1(N), \varepsilon\big)$ be a classical newform of weight $k \in \mathbb{N}_{\geqslant 2}$, level $N \in \mathbb{N}_{\geqslant 1}$ and nebentypus ε. Jean-Pierre Serre conjectured and Pierre Deligne proved in [Del71] that for every finite prime $\mathfrak{l}$ of the number field $K_f = \mathbb{Q}(a_n,\ n \geqslant 2)$ spanned by the coefficients a_n of the q-expansion of f at infinity, there exists a Galois representation

$$\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathbb{Z}_{K_{f,\mathfrak{l}}})$$

which is unramified outside ℓN and such that the image of any Frobenius element at $p \nmid \ell N$ has characteristic polynomial $x^2 - a_p x + \varepsilon(p)p^{k-1} \in \mathbb{Z}_{K_{f,\mathfrak{l}}}[x]$, where $\mathbb{Z}_{K_{f,\mathfrak{l}}}$ denotes the $\mathfrak{l}$-adic completion of the ring of integers $\mathbb{Z}_{K_f}$ of K_f, and ℓ is the rational prime lying below $\mathfrak{l}$.

Let $\mathbb{F}_\mathfrak{l}$ be the residue field of $\mathfrak{l}$. By reducing the above $\mathfrak{l}$-adic Galois representation modulo $\mathfrak{l}$, we get a modulo $\mathfrak{l}$ Galois representation

$$\rho_{f,\mathfrak{l}} \colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathbb{F}_\mathfrak{l}),$$

which is unramified outside ℓN and such that the image of any Frobenius element at $p \nmid \ell N$ has characteristic polynomial $x^2 - a_p x + \varepsilon(p)p^{k-1} \in \mathbb{F}_\mathfrak{l}[x]$. In particular, the trace of this image is a_p mod $\mathfrak{l}$.

In [Mas13], we described an algorithm based on ideas from the book [CE11] edited by Jean-Marc Couveignes and Bas Edixhoven to compute such modulo $\mathfrak{l}$ Galois representations, provided that the image of the Galois representation contains $\mathrm{SL}_2(\mathbb{F}_\mathfrak{l})$, that $k < \ell$, and that $\mathfrak{l}$ has inertia degree 1, so that $\mathbb{F}_\mathfrak{l} = \mathbb{F}_\ell$. This gives a way to quickly compute the coefficients a_p modulo $\mathfrak{l}$ for huge primes p.

The condition that the image of the Galois representation contain $\mathrm{SL}_2(\mathbb{F}_\mathfrak{l})$ is a very weak one. Indeed, by [Rib85, theorem 2.1] and [Swi72, lemma 2], for any non-CM newform f (and in particular for any newform f of level 1), the image of the representation $\rho_{f,\mathfrak{l}}$ contains $\mathrm{SL}_2(\mathbb{F}_\mathfrak{l})$ for almost every $\mathfrak{l}$. The finitely many $\mathfrak{l}$ for which $\mathrm{SL}_2(\mathbb{F}_\mathfrak{l}) \not\subset \mathrm{Im}\,\rho_{f,\mathfrak{l}}$ are called *exceptional primes* for f, and we exclude them. They were explicitly determined by Sir Peter Swinnerton-Dyer in [Swi72] for the known[1] newforms f of level 1 whose coefficients a_n are rational. In our case, this means we exclude $\mathfrak{l} = 23$ for $f = \Delta$ and $\mathfrak{l} = 31$ for $f = E_4\Delta$ (cf. the notations of section 3 below).

[1] According to Maeda's conjecture (cf [FW02]), there are only 6 such forms: Δ, $E_4\Delta$, $E_6\Delta$, $E_8\Delta$, $E_{10}\Delta$ and $E_{14}\Delta$ in the notation of section 3 below, of respective weights 12, 16, 18, 20, 22 and 26.

This algorithm relies on the fact that if $k < \ell$, then the Galois representation $\rho_{f,\mathfrak{l}}$ is afforded with multiplicity 1 by a subspace $V_{f,\mathfrak{l}}$ of the ℓ-torsion of the jacobian $J_1(\ell N)$ of the modular curve $X_1(\ell N)$ under the natural $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-action, cf [Gro90] and [Mas13, section 1].

The algorithm first computes the number field $L = \overline{\mathbb{Q}}^{\mathrm{Ker}\,\rho_{f,\mathfrak{l}}}$ cut out by the Galois representation, by evaluating a well-chosen function $\alpha \in \mathbb{Q}\big(J_1(\ell N)\big)$ in the nonzero points of $V_{f,\mathfrak{l}}$ and forming the polynomial

$$F(X) = \prod_{\substack{x \in V_{f,\mathfrak{l}} \\ x \neq 0}} \big(X - \alpha(x)\big) \in \mathbb{Q}[X]$$

of degree $\ell^2 - 1$ whose decomposition field is L. The algorithm then uses a method from T. and V. Dokchitser (cf [Dok10]) to compute the image of the Frobenius element at p given a rational prime $p \nmid \ell N$. Since such a Frobenius element is defined only up to conjugation, the output is a similarity class in $\mathrm{GL}_2(\mathbb{F}_\mathfrak{l})$.

2 Reducing the polynomials

Unfortunately, the coefficients of the polynomial $F(X)$ tend to have larger and larger height as ℓ grows. More precisely, the following table, which shows the genus $g = \frac{(\ell-5)(\ell-7)}{24}$ of the modular curves $X_1(\ell)$ and the rough number h of decimal digits in the common denominator of the polynomials $F(X)$ associated to newforms of level $N = 1$ (cf the Tables section below) which we computed using the algorithm described in [Mas13], seems to indicate the heuristic $h \approx g^{2.5}$:

ℓ	g	h
11	1	0
13	2	5
17	5	50
19	7	150
23	12	500
29	22	1800
31	26	2500

While this is rather harmless for $l \leqslant 17$, it makes the Dokchitser's method intractable as soon as $\ell \geqslant 29$. It is thus necessary to reduce this polynomial, that is to say to compute another polynomial whose splitting field is isomorphic to the splitting field of $F(X)$ but whose coefficients are much nicer. An algorithm to perform this task based on LLL lattice reduction is described in [Coh93, section 4.4.2] and implemented in [Pari/GP] under the name `polred`. However, the polynomial $F(X)$ has degree $\ell^2 - 1$ and tends to have ugly coefficients, and this is too much for `polred` to be practical, even for small values of ℓ. Indeed, the fact that `polred` is based on LLL reduction means that its execution time is especially sensitive to the degree of the polynomial.

On the other hand, it would be possible to apply the `polred` algorithm to the polynomial

$$F^{\mathrm{proj}}(X) = \prod_{W \in \mathbb{P}V_{f,\mathfrak{l}}} \left(X - \sum_{\substack{x \in W \\ x \neq 0}} \alpha(x) \right) \in \mathbb{Q}[X]$$

whose splitting field is the number field L^{proj} cut out by the *projective* Galois representation

$$\rho_{f,\mathfrak{l}}^{\mathrm{proj}} \colon \ \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \xrightarrow{\rho_{f,\mathfrak{l}}} \mathrm{GL}_2(\mathbb{F}_\ell) \longrightarrow\!\!\!\!\!\rightarrow \mathrm{PGL}_2(\mathbb{F}_\ell)$$

since the degree of this polynomial is only $\ell + 1$, but this representation does not contain enough information to recover the values of a_p mod $\mathfrak{l}$.

However, we noted in [Mas13, section 3.7.2] that if $S \subset \mathbb{F}_\ell^*$ denotes the largest subgroup of $\mathbb{F}_\ell^*$ **not** containing -1, then the knowledge of the quotient representation

$$\rho_{f,\mathfrak{l}}^{S} \colon \ \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \xrightarrow{\rho_{f,\mathfrak{l}}} \mathrm{GL}_2(\mathbb{F}_\ell) \longrightarrow\!\!\!\!\!\rightarrow \mathrm{GL}_2(\mathbb{F}_\ell)/S \ ,$$

combined with the fact that the image in $\mathrm{GL}_2(\mathbb{F}_\ell)$ of a Frobenius element at p has determinant $p^{k-1}\varepsilon(p)$ mod $\mathfrak{l}$, is enough to recover the values of a_p mod $\mathfrak{l}$. It is

therefore enough for our purpose to compute this quotient representation, by first forming the polynomial

$$F^S(X) = \prod_{\substack{Sx \in V_{f,\mathfrak{l}}/S \\ x \neq 0}} \left(X - \sum_{s \in S} \alpha(sx) \right) \in \mathbb{Q}[X],$$

whose splitting field is the number field L^S cut out by $\rho^S_{f,\mathfrak{l}}$, and then to apply the Dokchitsers' method on it in order to compute the images of the Frobenius elements by $\rho^S_{f,\mathfrak{l}}$, cf [Mas13, section 3.7.2].

This is practical provided that we manage to apply the `polred` algorithm to $F^S(X)$, that is to say if the degree of $F^S(X)$ is not too large. Let $\ell - 1 = 2^r s$ with $s \in \mathbb{N}$ odd. Since we have $|S| = s$, the degree of F^S is $2^r(\ell+1)$, so we can `polred` F^S in the cases $\ell = 19$ or 23, but the cases $\ell = 29$ or 31 remain impractical.

For these remaining cases, Bill Allombert suggested to the author that one can still reduce $F^S(X)$ in several steps, as we now explain. Since $\mathbb{F}_\ell^*$ is cyclic, we have a filtration

$$\mathbb{F}_\ell^* = S_0 \underset{2}{\supset} S_1 \underset{2}{\supset} \cdots \underset{2}{\supset} S_r = S$$

with $[S_i : S_{i+1}] = 2$ for all i, namely

$$S_i = \mathrm{Im} \begin{pmatrix} \mathbb{F}_\ell^* & \longrightarrow & \mathbb{F}_\ell^* \\ x & \longmapsto & x^{2^i} \end{pmatrix}.$$

For each $i \leqslant r$, let us define

$$F_i(X) = \prod_{\substack{S_i x \in V_{f,\mathfrak{l}}/S_i \\ x \neq 0}} \left(X - \sum_{s \in S_i} \alpha(sx) \right) \in \mathbb{Q}[X],$$

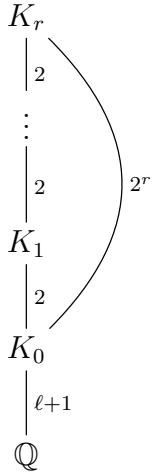
$$K_i = \mathbb{Q}[X]/F_i(X),$$

and L_i = normal closure of K_i = the number field cut out by the quotient representation

$$\rho^{S_i}_{f,\mathfrak{l}} \colon \ \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \xrightarrow{\rho_{f,\mathfrak{l}}} \mathrm{GL}_2(\mathbb{F}_\ell) \longrightarrow\!\!\!\!\!\rightarrow \mathrm{GL}_2(\mathbb{F}_\ell)/S_i \ .$$

In particular, we have $\rho^{S_0}_{f,\mathfrak{l}} = \rho^{\mathrm{proj}}_{f,\mathfrak{l}}$, $L_0 = L^{\mathrm{proj}}$, and we are looking for a nice model of K_r.

The fields K_i fit in an extension tower



and we are going to `polred` the polynomials $F_i(X)$ along this tower recursively from bottom up, as we now explain.

First, we apply directly the `polred` algorithm to $F_0(X) = F^{\mathrm{proj}}(X)$. Since the degree of this polynomial is only $\ell + 1$, this is amenable, as mentioned above.

Then, assuming we have managed to reduce $F_i(X)$, we have a nice model for $K_i = \mathbb{Q}[X]/F_i(X)$, so we can factor $F_{i+1}(X)$ in $K_i[X]$. Since the extension $K_{i+1} = \mathbb{Q}[X]/F_{i+1}(X)$ is quadratic over K_i, there must be at least one factor of degree 2. Let $G_{i+1}(X)$ be one of those, and let $\Delta_i \in K_i$ be its discriminant, so that we have

$$K_{i+1} \simeq K_i[X]/G_{i+1}(X) \simeq K_i\big(\sqrt{\Delta_i}\big).$$

In order to complete the recursion, all we have to do is to strip Δ_i from the largest square factor we can find, say $\Delta_i = A_i^2\delta_i$ with $A_i, \delta_i \in K_i$ and δ_i as small as possible. Indeed we then have $K_{i+1} = K_i\big(\sqrt{\delta_i}\big)$, and actually even $K_{i+1} = \mathbb{Q}\big(\sqrt{\delta_i}\big)$ unless we are very unlucky[2], so that if we denote by $\chi_i(X) \in \mathbb{Q}[X]$ the characteristic polynomial of δ_i, then we have

$$K_{i+1} \simeq \mathbb{Q}[X]/\chi_i(X^2),$$

so that $\chi_i(X^2)$ is a reduced version of F_{i+1}. If its degree and coefficients are not too big, we can even apply the `polred` algorithm to this polynomial in order to further reduce it, which is what we do in practice.

In order to write $\Delta_i = A_i^2\delta_i$, we would like to factor Δ_i in K_i, but even if K_i is principal, this is not amenable whatsoever. We can however consider the ideal generated by Δ_i in K_i, and remove its ℓN-part. The fractional ideal $\mathfrak{B}_i$ we obtain must then be a perfect square, since K_{i+1} is unramified outside ℓN (since L is), and the very efficient `idealsqrt` script from [BS14] can explicitly factor it into $\mathfrak{B}_i = \mathfrak{A}_i^2$. If A_i denotes an element in $\mathfrak{A}_i$ close to being a generator of $\mathfrak{A}_i$ (an actual generator, if amenable, would be even better), then $\delta_i := \Delta_i/A_i^2$ must be small.

[2]In practice, the case $K_{i+1} \supsetneq \mathbb{Q}\big(\sqrt{\delta_i}\big)$ has never happened to us. Should it happen, it can be corrected by multiplying δ_i by the square of an (hopefully small) element in K_i.

3 The tables

Notation

Following the tradition, we define

$$E_4 = 1 + 240\sum_{n=1}^{+\infty}\sigma_3(n)q^n, \quad E_6 = 1 - 504\sum_{n=1}^{+\infty}\sigma_5(n)q^n, \quad \text{and } \Delta = \frac{E_4^3 - E_6^2}{1728},$$

where $\sigma_k(n) = \sum_{0<d|n} d^k$.

We computed the Galois representations modulo the primes ℓ ranging from 11 to 31 and attached to the newforms $f \in S_k(1)$ of level $N = 1$ and of weight $k < \ell$. According to Maeda's conjecture, for each weight k, there is only one newform in $S_k(1)$ up to $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-conjugation. This conjecture has been verified in [FW02] for k up to 2000, and since we work with newforms of level 1 and weight k up to only 30 (because of the condition $k < \ell$), we may denote without ambiguity one of the newforms in $S_k(1)$ by f_k, and the coefficients of its q-expansion at infinity by $\tau_k(n)$. Then, for each k, the newform f_k and the sequence $\big(\tau_k(n)\big)_{n\geqslant 2}$ are well-defined up to $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-action, and the newforms in $S_k(1)$ are the $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-conjugates of

$$f_k = q + \sum_{n=2}^{+\infty}\tau_k(n)q^n.$$

Thus for instance we have $f_{12} = \Delta$, $\tau_{12} = \tau$ is Ramanujan's τ-function, $f_{16} = E_4\Delta = q + \sum_{n=2}^{+\infty}\tau_{16}(n)q^n$ is the only newform of level 1 and weight 16, and so on.

For each Galois representation $\rho_{f,\mathfrak{l}}$, we denote by L the number field it cuts off, and we give the image of the Frobenius element $\left(\frac{L/\mathbb{Q}}{p}\right)$ at p for the 40 first primes p above 10^{1000}. Since these p are unramified, these Frobenius elements are well-defined up to conjugacy, so their images are well-defined up to similarity. Instead of representing a similarity class in $\mathrm{GL}_2(\mathbb{F}_\mathfrak{l})$ by a matrix as we did in [Mas13], we deemed it more elegant to give its *minimal* polynomial in factored form over $\mathbb{F}_\mathfrak{l}$. As we are dealing with matrices of size 2, this is a faithful representation. Indeed, recall that $\mathrm{GL}_2(\mathbb{F}_\ell)$ splits into similarity classes as follows:

Type of class	Representative	Minimal polynomial	no of classes	no of elements in class
Scalar	$\left[\begin{smallmatrix}\lambda & 0\\ 0 & \lambda\end{smallmatrix}\right]$	$x-\lambda$	$\ell-1$	1
Split semisimple	$\left[\begin{smallmatrix}\lambda & 0\\ 0 & \mu\end{smallmatrix}\right]$	$(x-\lambda)(x-\mu)$	$\frac{(\ell-1)(\ell-2)}{2}$	$\ell(\ell+1)$
Non-split semisimple	$\left[\begin{smallmatrix}0 & -n\\ 1 & t\end{smallmatrix}\right]$	x^2-tx+n irreducible over $\mathbb{F}_\ell$	$\frac{\ell(\ell-1)}{2}$	$\ell(\ell-1)$
Non-semisimple	$\left[\begin{smallmatrix}\lambda & 1\\ 0 & \lambda\end{smallmatrix}\right]$	$(x-\lambda)^2$	$\ell-1$	$(\ell+1)(\ell-1)$

For each p, we also give the trace of the image of $\left(\frac{L/\mathbb{Q}}{p}\right)$, which is none other than the reduction modulo $\mathfrak{l}$ of the coefficient a_p of the newform f.

$\ell = 11$

$$f_{12} = \Delta = \sum_{n=1}^{+\infty} \tau(n) q^n = q - 24q^2 + 252q^3 + O(q^4)$$

p	Similarity class of $\left(\frac{L/\mathbb{Q}}{p}\right)$	$\tau(p) \bmod 11$
$10^{1000} + 453$	$(x-9)(x-4)$	2
$10^{1000} + 1357$	$(x-8)(x-2)$	10
$10^{1000} + 2713$	$x^2 + x + 8$	10
$10^{1000} + 4351$	$(x-6)(x-3)$	9
$10^{1000} + 5733$	$x^2 + 3x + 3$	8
$10^{1000} + 7383$	$x^2 + 3x + 3$	8
$10^{1000} + 10401$	$(x-8)(x-5)$	2
$10^{1000} + 11979$	$x^2 + 1$	0
$10^{1000} + 17557$	$(x-10)(x-9)$	8
$10^{1000} + 21567$	$x^2 + 10x + 8$	1
$10^{1000} + 22273$	$(x-9)(x-6)$	4
$10^{1000} + 24493$	$(x-8)(x-1)$	9
$10^{1000} + 25947$	$(x-9)(x-6)$	4
$10^{1000} + 27057$	$x^2 + 4x + 9$	7
$10^{1000} + 29737$	$(x-9)(x-3)$	1
$10^{1000} + 41599$	$x^2 + 9$	0
$10^{1000} + 43789$	$x^2 + 6x + 10$	5
$10^{1000} + 46227$	$(x-7)(x-4)$	0
$10^{1000} + 46339$	$(x-8)(x-1)$	9
$10^{1000} + 52423$	$(x-3)^2$	6
$10^{1000} + 55831$	$x^2 + 10x + 7$	1
$10^{1000} + 57867$	$(x-8)(x-1)$	9
$10^{1000} + 59743$	$(x-3)(x-1)$	4
$10^{1000} + 61053$	$(x-9)^2$	7
$10^{1000} + 61353$	$x^2 + x + 7$	10
$10^{1000} + 63729$	$x^2 + x + 7$	10
$10^{1000} + 64047$	$(x-3)(x-2)$	5
$10^{1000} + 64749$	$(x-10)(x-7)$	6
$10^{1000} + 68139$	$x^2 + 2x + 6$	9
$10^{1000} + 68367$	$(x-3)(x-1)$	4
$10^{1000} + 70897$	$(x-10)(x-8)$	7
$10^{1000} + 72237$	$(x-4)(x-3)$	7
$10^{1000} + 77611$	$(x-8)(x-5)$	2
$10^{1000} + 78199$	$(x-6)(x-2)$	8
$10^{1000} + 79237$	$(x-5)(x-1)$	6
$10^{1000} + 79767$	$x^2 + 4x + 7$	7
$10^{1000} + 82767$	$x^2 + 2x + 4$	9
$10^{1000} + 93559$	$(x-4)^2$	8
$10^{1000} + 95107$	$(x-10)(x-9)$	8
$10^{1000} + 100003$	$(x-9)(x-4)$	2

$\ell = 13$

$$f_{12} = \Delta = \sum_{n=1}^{+\infty} \tau(n) q^n = q - 24q^2 + 252q^3 + O(q^4)$$

p	Similarity class of $\left(\frac{L/\mathbb{Q}}{p}\right)$	$\tau(p)$ mod 13
$10^{1000} + 453$	$x^2 + 3x + 1$	10
$10^{1000} + 1357$	$(x - 10)(x - 7)$	4
$10^{1000} + 2713$	$x^2 + 12x + 12$	1
$10^{1000} + 4351$	$x^2 + x + 12$	12
$10^{1000} + 5733$	$(x - 12)(x - 4)$	3
$10^{1000} + 7383$	$x^2 + 6x + 7$	7
$10^{1000} + 10401$	$(x - 5)(x - 2)$	7
$10^{1000} + 11979$	$(x - 9)^2$	5
$10^{1000} + 17557$	$x^2 + 6x + 4$	7
$10^{1000} + 21567$	$x^2 + 5x + 9$	8
$10^{1000} + 22273$	$(x - 10)(x - 8)$	5
$10^{1000} + 24493$	$x^2 + 8x + 10$	5
$10^{1000} + 25947$	$x^2 + 10x + 7$	3
$10^{1000} + 27057$	$(x - 7)(x - 4)$	11
$10^{1000} + 29737$	$x^2 + x + 3$	12
$10^{1000} + 41599$	$(x - 11)(x - 3)$	1
$10^{1000} + 43789$	$(x - 10)(x - 7)$	4
$10^{1000} + 46227$	$x^2 + 10x + 7$	3
$10^{1000} + 46339$	$(x - 8)(x - 7)$	2
$10^{1000} + 52423$	$(x - 10)(x - 3)$	0
$10^{1000} + 55831$	$(x - 4)(x - 3)$	7
$10^{1000} + 57867$	$(x - 2)(x - 1)$	3
$10^{1000} + 59743$	$x^2 + 6$	0
$10^{1000} + 61053$	$x^2 + x + 5$	12
$10^{1000} + 61353$	$(x - 11)(x - 5)$	3
$10^{1000} + 63729$	$(x - 11)(x - 1)$	12
$10^{1000} + 64047$	$(x - 10)(x - 9)$	6
$10^{1000} + 64749$	$(x - 4)(x - 3)$	7
$10^{1000} + 68139$	$x^2 + 6x + 3$	7
$10^{1000} + 68367$	$(x - 7)(x - 5)$	12
$10^{1000} + 70897$	$(x - 12)(x - 7)$	6
$10^{1000} + 72237$	$x^2 + 11x + 12$	2
$10^{1000} + 77611$	$x^2 + 5x + 10$	8
$10^{1000} + 78199$	$(x - 7)(x - 4)$	11
$10^{1000} + 79237$	$(x - 4)(x - 2)$	6
$10^{1000} + 79767$	$x^2 + 7x + 7$	6
$10^{1000} + 82767$	$x^2 + 9x + 12$	4
$10^{1000} + 93559$	$x^2 + 8x + 1$	5
$10^{1000} + 95107$	$x^2 + 10x + 7$	3
$10^{1000} + 100003$	$x^2 + 6x + 4$	7

$\ell = 17$

$$f_{12} = \Delta = \sum_{n=1}^{+\infty} \tau(n) q^n = q - 24q^2 + 252q^3 + O(q^4)$$

p	Similarity class of $\left(\frac{L/\mathbb{Q}}{p}\right)$	$\tau(p) \bmod 17$
$10^{1000} + 453$	$x^2 + 3$	0
$10^{1000} + 1357$	$(x - 15)^2$	13
$10^{1000} + 2713$	$(x - 14)(x - 12)$	9
$10^{1000} + 4351$	$(x - 10)(x - 6)$	16
$10^{1000} + 5733$	$(x - 6)(x - 4)$	10
$10^{1000} + 7383$	$(x - 15)(x - 2)$	0
$10^{1000} + 10401$	$(x - 7)(x - 3)$	10
$10^{1000} + 11979$	$x^2 + 6x + 3$	11
$10^{1000} + 17557$	$x^2 + 11x + 6$	6
$10^{1000} + 21567$	$x^2 + 16x + 3$	1
$10^{1000} + 22273$	$x^2 + 16x + 8$	1
$10^{1000} + 24493$	$x^2 + 8x + 6$	9
$10^{1000} + 25947$	$x^2 + 2x + 13$	15
$10^{1000} + 27057$	$(x - 16)(x - 2)$	1
$10^{1000} + 29737$	$x^2 + 5x + 7$	12
$10^{1000} + 41599$	$x^2 + 6x + 16$	11
$10^{1000} + 43789$	$(x - 11)(x - 5)$	16
$10^{1000} + 46227$	$x^2 + 4x + 7$	13
$10^{1000} + 46339$	$(x - 14)(x - 10)$	7
$10^{1000} + 52423$	$(x - 16)(x - 5)$	4
$10^{1000} + 55831$	$x^2 + 14x + 8$	3
$10^{1000} + 57867$	$x^2 + 8x + 9$	9
$10^{1000} + 59743$	$(x - 14)(x - 7)$	4
$10^{1000} + 61053$	$x^2 + 15x + 11$	2
$10^{1000} + 61353$	$x^2 + 6x + 16$	11
$10^{1000} + 63729$	$x^2 + 6$	0
$10^{1000} + 64047$	$x^2 + 7x + 14$	10
$10^{1000} + 64749$	$(x - 6)(x - 1)$	7
$10^{1000} + 68139$	$(x - 11)(x - 10)$	4
$10^{1000} + 68367$	$(x - 16)(x - 2)$	1
$10^{1000} + 70897$	$x^2 + 5x + 5$	12
$10^{1000} + 72237$	$x^2 + 7$	0
$10^{1000} + 77611$	$x^2 + 15x + 11$	2
$10^{1000} + 78199$	$(x - 16)(x - 8)$	7
$10^{1000} + 79237$	$(x - 10)(x - 5)$	15
$10^{1000} + 79767$	$(x - 8)(x - 1)$	9
$10^{1000} + 82767$	$x^2 + 16x + 3$	1
$10^{1000} + 93559$	$x^2 + 5x + 14$	12
$10^{1000} + 95107$	$(x - 11)^2$	5
$10^{1000} + 100003$	$(x - 14)(x - 5)$	2

$$f_{16} = E_4\Delta = \sum_{n=1}^{+\infty} \tau_{16}(n)q^n = q + 216q^2 - 3348q^3 + O(q^4)$$

p	Similarity class of $\left(\frac{L/\mathbb{Q}}{p}\right)$	$\tau_{16}(p)$ mod 17
$10^{1000} + 453$	$x^2 + 5x + 12$	12
$10^{1000} + 1357$	$x^2 + 3x + 4$	14
$10^{1000} + 2713$	$x^2 + 8x + 2$	9
$10^{1000} + 4351$	$x^2 + 14x + 8$	3
$10^{1000} + 5733$	$x^2 + 11x + 6$	6
$10^{1000} + 7383$	$(x - 8)^2$	16
$10^{1000} + 10401$	$(x - 16)(x - 13)$	12
$10^{1000} + 11979$	$(x - 9)(x - 7)$	16
$10^{1000} + 17557$	$(x - 5)(x - 2)$	7
$10^{1000} + 21567$	$x^2 + 12x + 12$	5
$10^{1000} + 22273$	$x^2 + 13x + 9$	4
$10^{1000} + 24493$	$x^2 + 10$	0
$10^{1000} + 25947$	$(x - 16)(x - 4)$	3
$10^{1000} + 27057$	$(x - 10)(x - 7)$	0
$10^{1000} + 29737$	$x^2 + 9x + 6$	8
$10^{1000} + 41599$	$x^2 + 4x + 16$	13
$10^{1000} + 43789$	$(x - 4)(x - 1)$	5
$10^{1000} + 46227$	$(x - 12)(x - 9)$	4
$10^{1000} + 46339$	$x^2 + 15x + 4$	2
$10^{1000} + 52423$	$(x - 11)(x - 9)$	3
$10^{1000} + 55831$	$x^2 + 9x + 9$	8
$10^{1000} + 57867$	$x^2 + 12x + 8$	5
$10^{1000} + 59743$	$(x - 8)^2$	16
$10^{1000} + 61053$	$(x - 15)(x - 5)$	3
$10^{1000} + 61353$	$x^2 + 16x + 16$	1
$10^{1000} + 63729$	$x^2 + 14x + 10$	3
$10^{1000} + 64047$	$x^2 + 12x + 5$	5
$10^{1000} + 64749$	$x^2 + 10$	0
$10^{1000} + 68139$	$(x - 10)(x - 6)$	16
$10^{1000} + 68367$	$x^2 + 8x + 2$	9
$10^{1000} + 70897$	$(x - 16)(x - 14)$	13
$10^{1000} + 72237$	$(x - 13)(x - 7)$	3
$10^{1000} + 77611$	$(x - 6)(x - 4)$	10
$10^{1000} + 78199$	$(x - 8)(x - 1)$	9
$10^{1000} + 79237$	$x^2 + 13x + 16$	4
$10^{1000} + 79767$	$x^2 + 4x + 9$	13
$10^{1000} + 82767$	$x^2 + 5x + 12$	12
$10^{1000} + 93559$	$x^2 + 5$	0
$10^{1000} + 95107$	$(x - 7)^2$	14
$10^{1000} + 100003$	$(x - 10)^2$	3

$\ell = 19$

$$f_{12} = \Delta = \sum_{n=1}^{+\infty} \tau(n) q^n = q - 24q^2 + 252q^3 + O(q^4)$$

p	Similarity class of $\left(\frac{L/\mathbb{Q}}{p}\right)$	$\tau(p) \bmod 19$
$10^{1000} + 453$	$(x-15)(x-10)$	6
$10^{1000} + 1357$	$(x-17)^2$	15
$10^{1000} + 2713$	$(x-11)(x-4)$	15
$10^{1000} + 4351$	$(x-6)(x-4)$	10
$10^{1000} + 5733$	$(x-16)(x-1)$	17
$10^{1000} + 7383$	$(x-1)^2$	2
$10^{1000} + 10401$	$x^2 + 11x + 4$	8
$10^{1000} + 11979$	$(x-16)(x-13)$	10
$10^{1000} + 17557$	$x^2 + 8x + 14$	11
$10^{1000} + 21567$	$(x-11)^2$	3
$10^{1000} + 22273$	$(x-13)(x-1)$	14
$10^{1000} + 24493$	$(x-14)(x-10)$	5
$10^{1000} + 25947$	$x^2 + 14x + 15$	5
$10^{1000} + 27057$	$(x-10)(x-9)$	0
$10^{1000} + 29737$	$x^2 + 12x + 7$	7
$10^{1000} + 41599$	$(x-18)(x-15)$	14
$10^{1000} + 43789$	$(x-13)(x-11)$	5
$10^{1000} + 46227$	$x^2 + 5$	0
$10^{1000} + 46339$	$x^2 + x + 11$	18
$10^{1000} + 52423$	$x^2 + 7x + 7$	12
$10^{1000} + 55831$	$(x-16)(x-13)$	10
$10^{1000} + 57867$	$(x-17)(x-2)$	0
$10^{1000} + 59743$	$x^2 + 5x + 9$	14
$10^{1000} + 61053$	$x^2 + 9x + 3$	10
$10^{1000} + 61353$	$(x-14)(x-10)$	5
$10^{1000} + 63729$	$x^2 + 15x + 8$	4
$10^{1000} + 64047$	$(x-6)(x-5)$	11
$10^{1000} + 64749$	$(x-13)^2$	7
$10^{1000} + 68139$	$x^2 + 15x + 13$	4
$10^{1000} + 68367$	$(x-14)(x-5)$	0
$10^{1000} + 70897$	$(x-18)(x-15)$	14
$10^{1000} + 72237$	$(x-10)(x-5)$	15
$10^{1000} + 77611$	$x^2 + 13x + 6$	6
$10^{1000} + 78199$	$(x-15)^2$	11
$10^{1000} + 79237$	$x^2 + 12x + 9$	7
$10^{1000} + 79767$	$x^2 + 13x + 13$	6
$10^{1000} + 82767$	$x^2 + 3x + 8$	16
$10^{1000} + 93559$	$x^2 + 4x + 8$	15
$10^{1000} + 95107$	$x^2 + 13x + 15$	6
$10^{1000} + 100003$	$x^2 + 5x + 3$	14

$$f_{16} = E_4\Delta = \sum_{n=1}^{+\infty} \tau_{16}(n)q^n = q + 216q^2 - 3348q^3 + O(q^4)$$

p	Similarity class of $\left(\frac{L/\mathbb{Q}}{p}\right)$	$\tau_{16}(p)$ mod 19
$10^{1000} + 453$	$(x-15)(x-2)$	17
$10^{1000} + 1357$	$(x-18)(x-12)$	11
$10^{1000} + 2713$	$x^2 + 6x + 7$	13
$10^{1000} + 4351$	$x^2 + 9x + 11$	10
$10^{1000} + 5733$	$(x-17)(x-4)$	2
$10^{1000} + 7383$	$x^2 + 5x + 1$	14
$10^{1000} + 10401$	$x^2 + 13x + 7$	6
$10^{1000} + 11979$	$(x-16)(x-13)$	10
$10^{1000} + 17557$	$(x-9)(x-3)$	12
$10^{1000} + 21567$	$x^2 + 5x + 1$	14
$10^{1000} + 22273$	$(x-17)(x-13)$	11
$10^{1000} + 24493$	$(x-17)(x-9)$	7
$10^{1000} + 25947$	$(x-18)(x-7)$	6
$10^{1000} + 27057$	$x^2 + 5x + 8$	14
$10^{1000} + 29737$	$(x-13)(x-3)$	16
$10^{1000} + 41599$	$x^2 + 7x + 7$	12
$10^{1000} + 43789$	$x^2 + 9x + 12$	10
$10^{1000} + 46227$	$x^2 + 16x + 11$	3
$10^{1000} + 46339$	$(x-17)(x-9)$	7
$10^{1000} + 52423$	$(x-15)(x-14)$	10
$10^{1000} + 55831$	$(x-14)(x-4)$	18
$10^{1000} + 57867$	$x^2 + 18x + 12$	1
$10^{1000} + 59743$	$x^2 + 7$	0
$10^{1000} + 61053$	$(x-17)(x-15)$	13
$10^{1000} + 61353$	$(x-10)(x-2)$	12
$10^{1000} + 63729$	$x^2 + 16x + 18$	3
$10^{1000} + 64047$	$(x-10)(x-2)$	12
$10^{1000} + 64749$	$x^2 + 10x + 11$	9
$10^{1000} + 68139$	$(x-10)(x-5)$	15
$10^{1000} + 68367$	$(x-18)(x-7)$	6
$10^{1000} + 70897$	$x^2 + 6x + 7$	13
$10^{1000} + 72237$	$x^2 + 6x + 18$	13
$10^{1000} + 77611$	$x^2 + 13x + 7$	6
$10^{1000} + 78199$	$(x-7)^2$	14
$10^{1000} + 79237$	$(x-14)(x-10)$	5
$10^{1000} + 79767$	$(x-12)(x-1)$	13
$10^{1000} + 82767$	$(x-16)(x-13)$	10
$10^{1000} + 93559$	$x^2 + 2x + 18$	17
$10^{1000} + 95107$	$x^2 + 18x + 12$	1
$10^{1000} + 100003$	$(x-14)(x-6)$	1

$$f_{18} = E_6\Delta = \sum_{n=1}^{+\infty} \tau_{18}(n)q^n = q - 528q^2 - 4284q^3 + O(q^4)$$

p	Similarity class of $\left(\frac{L/\mathbb{Q}}{p}\right)$	$\tau_{18}(p) \bmod 19$
$10^{1000} + 453$	$(x-7)(x-5)$	12
$10^{1000} + 1357$	$(x-14)(x-2)$	16
$10^{1000} + 2713$	$(x-13)(x-12)$	6
$10^{1000} + 4351$	$(x-15)(x-10)$	6
$10^{1000} + 5733$	$(x-12)(x-2)$	14
$10^{1000} + 7383$	$x^2 + 8x + 1$	11
$10^{1000} + 10401$	$(x-17)(x-5)$	3
$10^{1000} + 11979$	$(x-15)(x-5)$	1
$10^{1000} + 17557$	$x^2 + x + 2$	18
$10^{1000} + 21567$	$x^2 + 9x + 7$	10
$10^{1000} + 22273$	$x^2 + 9x + 15$	10
$10^{1000} + 24493$	$(x-13)(x-2)$	15
$10^{1000} + 25947$	$(x-18)(x-9)$	8
$10^{1000} + 27057$	$x^2 + x + 2$	18
$10^{1000} + 29737$	$x^2 + 13x + 7$	6
$10^{1000} + 41599$	$x^2 + 9$	0
$10^{1000} + 43789$	$(x-16)(x-2)$	18
$10^{1000} + 46227$	$x^2 + 17x + 17$	2
$10^{1000} + 46339$	$x^2 + x + 11$	18
$10^{1000} + 52423$	$(x-7)(x-1)$	8
$10^{1000} + 55831$	$(x-18)(x-1)$	0
$10^{1000} + 57867$	$(x-16)(x-3)$	0
$10^{1000} + 59743$	$(x-6)(x-1)$	7
$10^{1000} + 61053$	$x^2 + 18x + 14$	1
$10^{1000} + 61353$	$x^2 + 17x + 7$	2
$10^{1000} + 63729$	$x^2 + 15x + 8$	4
$10^{1000} + 64047$	$(x-7)^2$	14
$10^{1000} + 64749$	$(x-7)(x-5)$	12
$10^{1000} + 68139$	$(x-5)(x-3)$	8
$10^{1000} + 68367$	$(x-9)(x-8)$	17
$10^{1000} + 70897$	$(x-16)^2$	13
$10^{1000} + 72237$	$x^2 + 14x + 12$	5
$10^{1000} + 77611$	$x^2 + 9x + 4$	10
$10^{1000} + 78199$	$(x-18)(x-14)$	13
$10^{1000} + 79237$	$(x-15)(x-8)$	4
$10^{1000} + 79767$	$(x-18)(x-4)$	3
$10^{1000} + 82767$	$(x-16)(x-10)$	7
$10^{1000} + 93559$	$x^2 + 4x + 8$	15
$10^{1000} + 95107$	$x^2 + 10x + 10$	9
$10^{1000} + 100003$	$(x-15)(x-6)$	2

$\ell = 23$

$$f_{16} = E_4\Delta = \sum_{n=1}^{+\infty} \tau_{16}(n)q^n = q + 216q^2 - 3348q^3 + O(q^4)$$

p	Similarity class of $\left(\frac{L/\mathbb{Q}}{p}\right)$	$\tau_{16}(p) \bmod 23$
$10^{1000} + 453$	$(x-15)(x-5)$	20
$10^{1000} + 1357$	$(x-19)(x-15)$	11
$10^{1000} + 2713$	$x^2 + 11x + 21$	12
$10^{1000} + 4351$	$x^2 + 7x + 11$	16
$10^{1000} + 5733$	$(x-18)(x-14)$	9
$10^{1000} + 7383$	$(x-13)(x-6)$	19
$10^{1000} + 10401$	$x^2 + 4x + 7$	19
$10^{1000} + 11979$	$(x-15)(x-7)$	22
$10^{1000} + 17557$	$x^2 + 8x + 1$	15
$10^{1000} + 21567$	$x^2 + 8x + 6$	15
$10^{1000} + 22273$	$(x-17)(x-5)$	22
$10^{1000} + 24493$	$(x-8)(x-5)$	13
$10^{1000} + 25947$	$(x-21)(x-13)$	11
$10^{1000} + 27057$	$(x-8)(x-2)$	10
$10^{1000} + 29737$	$x^2 + 12x + 17$	11
$10^{1000} + 41599$	$(x-20)(x-7)$	4
$10^{1000} + 43789$	$(x-15)^2$	7
$10^{1000} + 46227$	$(x-9)(x-2)$	11
$10^{1000} + 46339$	$(x-22)(x-18)$	17
$10^{1000} + 52423$	$(x-19)(x-6)$	2
$10^{1000} + 55831$	$x^2 + 4x + 12$	19
$10^{1000} + 57867$	$x^2 + 16x + 21$	7
$10^{1000} + 59743$	$(x-7)(x-6)$	13
$10^{1000} + 61053$	$x^2 + 21x + 3$	2
$10^{1000} + 61353$	$(x-11)(x-8)$	19
$10^{1000} + 63729$	$x^2 + 5x + 13$	18
$10^{1000} + 64047$	$(x-22)(x-21)$	20
$10^{1000} + 64749$	$x^2 + 16x + 11$	7
$10^{1000} + 68139$	$(x-18)(x-3)$	21
$10^{1000} + 68367$	$x^2 + 2x + 3$	21
$10^{1000} + 70897$	$x^2 + 21x + 3$	2
$10^{1000} + 72237$	$x^2 + 14x + 5$	9
$10^{1000} + 77611$	$x^2 + 14x + 16$	9
$10^{1000} + 78199$	$x^2 + 6x + 21$	17
$10^{1000} + 79237$	$x^2 + 9x + 4$	14
$10^{1000} + 79767$	$x^2 + 15x + 20$	8
$10^{1000} + 82767$	$(x-8)(x-1)$	9
$10^{1000} + 93559$	$x^2 + x + 10$	22
$10^{1000} + 95107$	$(x-15)(x-11)$	3
$10^{1000} + 100003$	$(x-14)(x-13)$	4

$$f_{18} = E_6\Delta = \sum_{n=1}^{+\infty} \tau_{18}(n)q^n = q - 528q^2 - 4284q^3 + O(q^4)$$

p	Similarity class of $\left(\frac{L/\mathbb{Q}}{p}\right)$	$\tau_{18}(p) \bmod 23$
$10^{1000} + 453$	$(x-18)(x-4)$	22
$10^{1000} + 1357$	$x^2 + 10x + 4$	13
$10^{1000} + 2713$	$x^2 + 13x + 10$	10
$10^{1000} + 4351$	$(x-6)(x-5)$	11
$10^{1000} + 5733$	$x^2 + x + 22$	22
$10^{1000} + 7383$	$(x-20)(x-14)$	11
$10^{1000} + 10401$	$(x-7)(x-4)$	11
$10^{1000} + 11979$	$(x-11)(x-5)$	16
$10^{1000} + 17557$	$x^2 + 7x + 1$	16
$10^{1000} + 21567$	$(x-15)(x-14)$	6
$10^{1000} + 22273$	$x^2 + 22x + 18$	1
$10^{1000} + 24493$	$(x-15)(x-9)$	1
$10^{1000} + 25947$	$(x-7)(x-3)$	10
$10^{1000} + 27057$	$x^2 + 5x + 18$	18
$10^{1000} + 29737$	$x^2 + 5x + 20$	18
$10^{1000} + 41599$	$(x-13)(x-1)$	14
$10^{1000} + 43789$	$x^2 + 8x + 6$	15
$10^{1000} + 46227$	$x^2 + 4x + 6$	19
$10^{1000} + 46339$	$(x-18)(x-15)$	10
$10^{1000} + 52423$	$x^2 + 15x + 22$	8
$10^{1000} + 55831$	$(x-17)(x-5)$	22
$10^{1000} + 57867$	$x^2 + 22x + 10$	1
$10^{1000} + 59743$	$x^2 + 13x + 15$	10
$10^{1000} + 61053$	$(x-20)(x-7)$	4
$10^{1000} + 61353$	$(x-15)(x-1)$	16
$10^{1000} + 63729$	$x^2 + 9$	0
$10^{1000} + 64047$	$(x-17)^2$	11
$10^{1000} + 64749$	$x^2 + 22x + 7$	1
$10^{1000} + 68139$	$(x-9)^2$	18
$10^{1000} + 68367$	$x^2 + 8x + 2$	15
$10^{1000} + 70897$	$(x-2)(x-1)$	3
$10^{1000} + 72237$	$(x-17)(x-1)$	18
$10^{1000} + 77611$	$(x-19)(x-7)$	3
$10^{1000} + 78199$	$(x-17)(x-6)$	0
$10^{1000} + 79237$	$x^2 + 4x + 8$	19
$10^{1000} + 79767$	$x^2 + 11x + 21$	12
$10^{1000} + 82767$	$x^2 + x + 12$	22
$10^{1000} + 93559$	$(x-10)(x-6)$	16
$10^{1000} + 95107$	$x^2 + 13x + 8$	10
$10^{1000} + 100003$	$(x-14)(x-4)$	18

$$f_{20} = E_8\Delta = \sum_{n=1}^{+\infty} \tau_{20}(n)q^n = q + 456q^2 + 50652q^3 + O(q^4)$$

p	Similarity class of $\left(\frac{L/\mathbb{Q}}{p}\right)$	$\tau_{20}(p)$ mod 23
$10^{1000} + 453$	$x^2 + 5x + 13$	18
$10^{1000} + 1357$	$x^2 + 22x + 12$	1
$10^{1000} + 2713$	$x^2 + 11x + 19$	12
$10^{1000} + 4351$	$(x - 22)(x - 6)$	5
$10^{1000} + 5733$	$x^2 + 22x + 22$	1
$10^{1000} + 7383$	$(x - 15)(x - 10)$	2
$10^{1000} + 10401$	$x^2 + 13x + 20$	10
$10^{1000} + 11979$	$x^2 + 10x + 8$	13
$10^{1000} + 17557$	$(x - 16)(x - 13)$	6
$10^{1000} + 21567$	$(x - 18)(x - 2)$	20
$10^{1000} + 22273$	$(x - 22)(x - 20)$	19
$10^{1000} + 24493$	$(x - 11)(x - 3)$	14
$10^{1000} + 25947$	$x^2 + 18x + 14$	5
$10^{1000} + 27057$	$x^2 + 16x + 3$	7
$10^{1000} + 29737$	$x^2 + 22x + 10$	1
$10^{1000} + 41599$	$(x - 22)(x - 19)$	18
$10^{1000} + 43789$	$x^2 + 2$	0
$10^{1000} + 46227$	$(x - 14)(x - 10)$	1
$10^{1000} + 46339$	$(x - 18)(x - 5)$	0
$10^{1000} + 52423$	$(x - 21)(x - 12)$	10
$10^{1000} + 55831$	$(x - 21)(x - 20)$	18
$10^{1000} + 57867$	$(x - 22)(x - 4)$	3
$10^{1000} + 59743$	$(x - 11)(x - 9)$	20
$10^{1000} + 61053$	$x^2 + 9x + 9$	14
$10^{1000} + 61353$	$(x - 22)(x - 16)$	15
$10^{1000} + 63729$	$x^2 + 19x + 8$	4
$10^{1000} + 64047$	$(x - 18)(x - 13)$	8
$10^{1000} + 64749$	$(x - 21)(x - 3)$	1
$10^{1000} + 68139$	$(x - 18)(x - 1)$	19
$10^{1000} + 68367$	$x^2 + x + 9$	22
$10^{1000} + 70897$	$x^2 + 21x + 9$	2
$10^{1000} + 72237$	$(x - 11)(x - 4)$	15
$10^{1000} + 77611$	$(x - 15)(x - 14)$	6
$10^{1000} + 78199$	$(x - 17)(x - 16)$	10
$10^{1000} + 79237$	$x^2 + 5x + 16$	18
$10^{1000} + 79767$	$x^2 + 18x + 14$	5
$10^{1000} + 82767$	$(x - 11)(x - 10)$	21
$10^{1000} + 93559$	$x^2 + 6x + 15$	17
$10^{1000} + 95107$	$(x - 19)^2$	15
$10^{1000} + 100003$	$x^2 + 15x + 19$	8

$$f_{22} = E_{10}\Delta = \sum_{n=1}^{+\infty} \tau_{22}(n)q^n = q - 288q^2 - 128844q^3 + O(q^4)$$

p	Similarity class of $\left(\frac{L/\mathbb{Q}}{p}\right)$	$\tau_{22}(p) \bmod 23$
$10^{1000} + 453$	$(x-19)(x-7)$	3
$10^{1000} + 1357$	$x^2 + 13$	0
$10^{1000} + 2713$	$x^2 + 8x + 20$	15
$10^{1000} + 4351$	$(x-16)(x-11)$	4
$10^{1000} + 5733$	$x^2 + 19x + 22$	4
$10^{1000} + 7383$	$(x-19)(x-14)$	10
$10^{1000} + 10401$	$(x-16)(x-5)$	21
$10^{1000} + 11979$	$(x-17)(x-15)$	9
$10^{1000} + 17557$	$(x-19)(x-17)$	13
$10^{1000} + 21567$	$(x-19)(x-7)$	3
$10^{1000} + 22273$	$x^2 + 14x + 12$	9
$10^{1000} + 24493$	$(x-7)(x-4)$	11
$10^{1000} + 25947$	$x^2 + 4x + 17$	19
$10^{1000} + 27057$	$x^2 + 3x + 12$	20
$10^{1000} + 29737$	$x^2 + 5x + 5$	18
$10^{1000} + 41599$	$(x-7)^2$	14
$10^{1000} + 43789$	$x^2 + 18x + 16$	5
$10^{1000} + 46227$	$x^2 + 19x + 16$	4
$10^{1000} + 46339$	$x^2 + 22x + 7$	1
$10^{1000} + 52423$	$(x-22)(x-1)$	0
$10^{1000} + 55831$	$x^2 + 12x + 8$	11
$10^{1000} + 57867$	$(x-17)(x-12)$	6
$10^{1000} + 59743$	$(x-21)(x-16)$	14
$10^{1000} + 61053$	$x^2 + 4x + 6$	19
$10^{1000} + 61353$	$(x-19)(x-8)$	4
$10^{1000} + 63729$	$(x-5)^2$	10
$10^{1000} + 64047$	$(x-12)(x-6)$	18
$10^{1000} + 64749$	$(x-13)(x-10)$	0
$10^{1000} + 68139$	$(x-21)^2$	19
$10^{1000} + 68367$	$(x-19)(x-10)$	6
$10^{1000} + 70897$	$x^2 + 14x + 6$	9
$10^{1000} + 72237$	$(x-20)(x-13)$	10
$10^{1000} + 77611$	$(x-4)(x-3)$	7
$10^{1000} + 78199$	$(x-14)(x-8)$	22
$10^{1000} + 79237$	$x^2 + 20x + 9$	3
$10^{1000} + 79767$	$x^2 + 8x + 17$	15
$10^{1000} + 82767$	$x^2 + 16x + 4$	7
$10^{1000} + 93559$	$(x-14)(x-13)$	4
$10^{1000} + 95107$	$(x-3)^2$	6
$10^{1000} + 100003$	$(x-19)(x-18)$	14

$\ell = 29$

$$f_{12} = \Delta = \sum_{n=1}^{+\infty} \tau(n) q^n = q - 24q^2 + 252q^3 + O(q^4)$$

p	Similarity class of $\left(\frac{L/\mathbb{Q}}{p}\right)$	$\tau(p) \bmod 29$
$10^{1000} + 453$	$x^2 + 8x + 24$	21
$10^{1000} + 1357$	$x^2 + 21x + 1$	8
$10^{1000} + 2713$	$x^2 + 18x + 20$	11
$10^{1000} + 4351$	$x^2 + 3$	0
$10^{1000} + 5733$	$(x - 20)(x - 2)$	22
$10^{1000} + 7383$	$(x - 19)(x - 10)$	0
$10^{1000} + 10401$	$(x - 7)(x - 2)$	9
$10^{1000} + 11979$	$x^2 + 22x + 22$	7
$10^{1000} + 17557$	$x^2 + 27$	0
$10^{1000} + 21567$	$(x - 23)(x - 3)$	26
$10^{1000} + 22273$	$x^2 + 15x + 3$	14
$10^{1000} + 24493$	$x^2 + 25x + 16$	4
$10^{1000} + 25947$	$(x - 27)(x - 15)$	13
$10^{1000} + 27057$	$x^2 + 22x + 23$	7
$10^{1000} + 29737$	$(x - 23)(x - 10)$	4
$10^{1000} + 41599$	$(x - 13)(x - 5)$	18
$10^{1000} + 43789$	$(x - 18)(x - 15)$	4
$10^{1000} + 46227$	$x^2 + 7x + 3$	22
$10^{1000} + 46339$	$(x - 26)(x - 8)$	5
$10^{1000} + 52423$	$(x - 17)(x - 16)$	4
$10^{1000} + 55831$	$x^2 + 21x + 4$	8
$10^{1000} + 57867$	$(x - 13)(x - 11)$	24
$10^{1000} + 59743$	$x^2 + 24x + 2$	5
$10^{1000} + 61053$	$x^2 + 18x + 21$	11
$10^{1000} + 61353$	$(x - 24)(x - 1)$	25
$10^{1000} + 63729$	$(x - 20)(x - 1)$	21
$10^{1000} + 64047$	$x^2 + 14x + 6$	15
$10^{1000} + 64749$	$x^2 + 14x + 28$	15
$10^{1000} + 68139$	$(x - 12)(x - 2)$	14
$10^{1000} + 68367$	$x^2 + 26x + 26$	3
$10^{1000} + 70897$	$x^2 + 12x + 28$	17
$10^{1000} + 72237$	$x^2 + 27x + 13$	2
$10^{1000} + 77611$	$(x - 14)(x - 13)$	27
$10^{1000} + 78199$	$(x - 17)(x - 14)$	2
$10^{1000} + 79237$	$x^2 + 28x + 25$	1
$10^{1000} + 79767$	$x^2 + 13x + 16$	16
$10^{1000} + 82767$	$(x - 27)(x - 13)$	11
$10^{1000} + 93559$	$x^2 + 13x + 17$	16
$10^{1000} + 95107$	$(x - 25)(x - 24)$	20
$10^{1000} + 100003$	$(x - 26)(x - 13)$	10

$$f_{16} = E_4\Delta = \sum_{n=1}^{+\infty} \tau_{16}(n)q^n = q + 216q^2 - 3348q^3 + O(q^4)$$

p	Similarity class of $\left(\frac{L/\mathbb{Q}}{p}\right)$	$\tau_{16}(p)$ mod 29
$10^{1000} + 453$	$x^2 + 16x + 25$	13
$10^{1000} + 1357$	$x^2 + 9x + 1$	20
$10^{1000} + 2713$	$(x - 23)(x - 1)$	24
$10^{1000} + 4351$	$x^2 + 18x + 21$	11
$10^{1000} + 5733$	$(x - 22)(x - 8)$	1
$10^{1000} + 7383$	$x^2 + x + 24$	28
$10^{1000} + 10401$	$(x - 17)(x - 7)$	24
$10^{1000} + 11979$	$x^2 + 26x + 9$	3
$10^{1000} + 17557$	$(x - 27)(x - 24)$	22
$10^{1000} + 21567$	$(x - 16)(x - 11)$	27
$10^{1000} + 22273$	$(x - 27)(x - 4)$	2
$10^{1000} + 24493$	$(x - 25)(x - 23)$	19
$10^{1000} + 25947$	$(x - 17)^2$	5
$10^{1000} + 27057$	$x^2 + 22x + 7$	7
$10^{1000} + 29737$	$x^2 + 10$	0
$10^{1000} + 41599$	$x^2 + 2x + 20$	27
$10^{1000} + 43789$	$x^2 + 19x + 6$	10
$10^{1000} + 46227$	$(x - 24)(x - 19)$	14
$10^{1000} + 46339$	$x^2 + 17x + 4$	12
$10^{1000} + 52423$	$(x - 26)(x - 9)$	6
$10^{1000} + 55831$	$(x - 17)(x - 11)$	28
$10^{1000} + 57867$	$(x - 27)(x - 24)$	22
$10^{1000} + 59743$	$x^2 + 28x + 19$	1
$10^{1000} + 61053$	$(x - 21)(x - 20)$	12
$10^{1000} + 61353$	$x^2 + 13x + 25$	16
$10^{1000} + 63729$	$(x - 28)(x - 6)$	5
$10^{1000} + 64047$	$(x - 23)(x - 6)$	0
$10^{1000} + 64749$	$(x - 24)(x - 6)$	1
$10^{1000} + 68139$	$(x - 24)^2$	19
$10^{1000} + 68367$	$(x - 26)(x - 7)$	4
$10^{1000} + 70897$	$x^2 + 15x + 28$	14
$10^{1000} + 72237$	$(x - 28)(x - 24)$	23
$10^{1000} + 77611$	$x^2 + 19x + 15$	10
$10^{1000} + 78199$	$(x - 10)(x - 8)$	18
$10^{1000} + 79237$	$(x - 25)^2$	21
$10^{1000} + 79767$	$x^2 + 17x + 24$	12
$10^{1000} + 82767$	$x^2 + 6x + 21$	23
$10^{1000} + 93559$	$(x - 24)(x - 14)$	9
$10^{1000} + 95107$	$x^2 + 6x + 23$	23
$10^{1000} + 100003$	$(x - 26)(x - 6)$	3

$$f_{18} = E_6\Delta = \sum_{n=1}^{+\infty} \tau_{18}(n)q^n = q - 528q^2 - 4284q^3 + O(q^4)$$

p	Similarity class of $\left(\frac{L/\mathbb{Q}}{p}\right)$	$\tau_{18}(p) \bmod 29$
$10^{1000} + 453$	$x^2 + 13x + 23$	16
$10^{1000} + 1357$	$(x - 22)(x - 4)$	26
$10^{1000} + 2713$	$x^2 + 16x + 16$	13
$10^{1000} + 4351$	$(x - 23)(x - 8)$	2
$10^{1000} + 5733$	$(x - 16)(x - 15)$	2
$10^{1000} + 7383$	$(x - 13)(x - 6)$	19
$10^{1000} + 10401$	$x^2 + 27x + 27$	2
$10^{1000} + 11979$	$x^2 + 10x + 4$	19
$10^{1000} + 17557$	$x^2 + 19x + 14$	10
$10^{1000} + 21567$	$(x - 27)(x - 25)$	23
$10^{1000} + 22273$	$(x - 27)(x - 24)$	22
$10^{1000} + 24493$	$x^2 + 6x + 20$	23
$10^{1000} + 25947$	$(x - 21)(x - 11)$	3
$10^{1000} + 27057$	$x^2 + 23x + 24$	6
$10^{1000} + 29737$	$(x - 23)(x - 17)$	11
$10^{1000} + 41599$	$(x - 18)(x - 3)$	21
$10^{1000} + 43789$	$x^2 + 8x + 13$	21
$10^{1000} + 46227$	$(x - 14)(x - 9)$	23
$10^{1000} + 46339$	$(x - 18)(x - 10)$	28
$10^{1000} + 52423$	$(x - 16)(x - 15)$	2
$10^{1000} + 55831$	$x^2 + 22x + 22$	7
$10^{1000} + 57867$	$x^2 + 13x + 14$	16
$10^{1000} + 59743$	$(x - 22)(x - 2)$	24
$10^{1000} + 61053$	$x^2 + 8x + 18$	21
$10^{1000} + 61353$	$(x - 11)(x - 10)$	21
$10^{1000} + 63729$	$(x - 12)(x - 11)$	23
$10^{1000} + 64047$	$(x - 23)(x - 4)$	27
$10^{1000} + 64749$	$(x - 19)(x - 3)$	22
$10^{1000} + 68139$	$x^2 + 4x + 23$	25
$10^{1000} + 68367$	$(x - 15)(x - 9)$	24
$10^{1000} + 70897$	$(x - 25)(x - 22)$	18
$10^{1000} + 72237$	$(x - 18)(x - 15)$	4
$10^{1000} + 77611$	$(x - 25)(x - 19)$	15
$10^{1000} + 78199$	$(x - 19)(x - 14)$	4
$10^{1000} + 79237$	$(x - 19)(x - 8)$	27
$10^{1000} + 79767$	$(x - 17)(x - 8)$	25
$10^{1000} + 82767$	$(x - 27)(x - 24)$	22
$10^{1000} + 93559$	$(x - 11)(x - 9)$	20
$10^{1000} + 95107$	$x^2 + 24x + 16$	5
$10^{1000} + 100003$	$x^2 + 7x + 26$	22

$$f_{20} = E_8\Delta = \sum_{n=1}^{+\infty} \tau_{20}(n)q^n = q + 456q^2 + 50652q^3 + O(q^4)$$

p	Similarity class of $\left(\frac{L/\mathbb{Q}}{p}\right)$	$\tau_{20}(p)$ mod 29
$10^{1000} + 453$	$x^2 + 23x + 20$	6
$10^{1000} + 1357$	$x^2 + 25x + 1$	4
$10^{1000} + 2713$	$x^2 + 25x + 25$	4
$10^{1000} + 4351$	$(x - 25)(x - 14)$	10
$10^{1000} + 5733$	$x^2 + 27x + 3$	2
$10^{1000} + 7383$	$x^2 + 28x + 7$	1
$10^{1000} + 10401$	$(x - 22)(x - 15)$	8
$10^{1000} + 11979$	$(x - 9)(x - 7)$	16
$10^{1000} + 17557$	$x^2 + 28x + 8$	1
$10^{1000} + 21567$	$(x - 17)(x - 7)$	24
$10^{1000} + 22273$	$x^2 + 14x + 2$	15
$10^{1000} + 24493$	$(x - 18)(x - 2)$	20
$10^{1000} + 25947$	$x^2 + 2x + 28$	27
$10^{1000} + 27057$	$(x - 19)(x - 10)$	0
$10^{1000} + 29737$	$x^2 + 8x + 8$	21
$10^{1000} + 41599$	$x^2 + x + 24$	28
$10^{1000} + 43789$	$(x - 13)(x - 7)$	20
$10^{1000} + 46227$	$(x - 10)(x - 6)$	16
$10^{1000} + 46339$	$(x - 22)(x - 7)$	0
$10^{1000} + 52423$	$x^2 + 15x + 3$	14
$10^{1000} + 55831$	$(x - 19)(x - 11)$	1
$10^{1000} + 57867$	$(x - 11)(x - 6)$	17
$10^{1000} + 59743$	$(x - 18)(x - 6)$	24
$10^{1000} + 61053$	$x^2 + 2x + 19$	27
$10^{1000} + 61353$	$(x - 28)(x - 9)$	8
$10^{1000} + 63729$	$x^2 + 16x + 25$	13
$10^{1000} + 64047$	$x^2 + 5x + 13$	24
$10^{1000} + 64749$	$x^2 + 15x + 28$	14
$10^{1000} + 68139$	$(x - 25)(x - 24)$	20
$10^{1000} + 68367$	$(x - 22)(x - 21)$	14
$10^{1000} + 70897$	$(x - 7)(x - 4)$	11
$10^{1000} + 72237$	$(x - 27)(x - 18)$	16
$10^{1000} + 77611$	$(x - 17)(x - 4)$	21
$10^{1000} + 78199$	$x^2 + 8x + 13$	21
$10^{1000} + 79237$	$(x - 17)(x - 15)$	3
$10^{1000} + 79767$	$(x - 24)(x - 16)$	11
$10^{1000} + 82767$	$x^2 + 15x + 2$	14
$10^{1000} + 93559$	$(x - 23)(x - 2)$	25
$10^{1000} + 95107$	$x^2 + 5x + 25$	24
$10^{1000} + 100003$	$x^2 + 13x + 14$	16

$$f_{22} = E_{10}\Delta = \sum_{n=1}^{+\infty} \tau_{22}(n)q^n = q - 288q^2 - 128844q^3 + O(q^4)$$

p	Similarity class of $\left(\frac{L/\mathbb{Q}}{p}\right)$	$\tau_{22}(p) \bmod 29$
$10^{1000} + 453$	$(x-17)(x-12)$	0
$10^{1000} + 1357$	$x^2 + 8x + 1$	21
$10^{1000} + 2713$	$(x-6)(x-5)$	11
$10^{1000} + 4351$	$(x-20)(x-18)$	9
$10^{1000} + 5733$	$(x-4)(x-3)$	7
$10^{1000} + 7383$	$(x-17)(x-12)$	0
$10^{1000} + 10401$	$x^2 + 4x + 12$	25
$10^{1000} + 11979$	$(x-19)(x-3)$	22
$10^{1000} + 17557$	$x^2 + 15x + 17$	14
$10^{1000} + 21567$	$x^2 + x + 12$	28
$10^{1000} + 22273$	$(x-28)(x-17)$	16
$10^{1000} + 24493$	$(x-27)(x-14)$	12
$10^{1000} + 25947$	$(x-18)(x-8)$	26
$10^{1000} + 27057$	$x^2 + 9x + 1$	20
$10^{1000} + 29737$	$(x-13)(x-8)$	21
$10^{1000} + 41599$	$(x-10)(x-3)$	13
$10^{1000} + 43789$	$(x-21)(x-11)$	3
$10^{1000} + 46227$	$(x-20)(x-18)$	9
$10^{1000} + 46339$	$(x-24)(x-6)$	1
$10^{1000} + 52423$	$x^2 + 14x + 12$	15
$10^{1000} + 55831$	$(x-16)(x-9)$	25
$10^{1000} + 57867$	$(x-20)(x-11)$	2
$10^{1000} + 59743$	$(x-4)(x-3)$	7
$10^{1000} + 61053$	$x^2 + 11x + 12$	18
$10^{1000} + 61353$	$(x-22)(x-4)$	26
$10^{1000} + 63729$	$(x-1)^2$	2
$10^{1000} + 64047$	$(x-21)(x-11)$	3
$10^{1000} + 64749$	$(x-19)(x-3)$	22
$10^{1000} + 68139$	$x^2 + 20x + 1$	9
$10^{1000} + 68367$	$(x-18)(x-9)$	27
$10^{1000} + 70897$	$(x-7)(x-4)$	11
$10^{1000} + 72237$	$x^2 + 2x + 28$	27
$10^{1000} + 77611$	$(x-15)(x-5)$	20
$10^{1000} + 78199$	$(x-12)^2$	24
$10^{1000} + 79237$	$x^2 + 24x + 1$	5
$10^{1000} + 79767$	$(x-11)(x-8)$	19
$10^{1000} + 82767$	$x^2 + 26x + 12$	3
$10^{1000} + 93559$	$(x-20)(x-18)$	9
$10^{1000} + 95107$	$x^2 + 8x + 1$	21
$10^{1000} + 100003$	$(x-10)(x-7)$	17

$$f_{26} = E_{14}\Delta = \sum_{n=1}^{+\infty} \tau_{26}(n)q^n = q - 48q^2 - 195804q^3 + O(q^4)$$

p	Similarity class of $\left(\frac{L/\mathbb{Q}}{p}\right)$	$\tau_{26}(p) \bmod 29$
$10^{1000} + 453$	$(x-16)^2$	3
$10^{1000} + 1357$	$x^2 + 24x + 1$	5
$10^{1000} + 2713$	$x^2 + 27x + 20$	2
$10^{1000} + 4351$	$x^2 + 8x + 26$	21
$10^{1000} + 5733$	$x^2 + 14x + 18$	15
$10^{1000} + 7383$	$(x-9)(x-5)$	14
$10^{1000} + 10401$	$x^2 + 4x + 15$	25
$10^{1000} + 11979$	$(x-15)^2$	1
$10^{1000} + 17557$	$(x-16)(x-11)$	27
$10^{1000} + 21567$	$(x-27)(x-20)$	18
$10^{1000} + 22273$	$(x-27)(x-16)$	14
$10^{1000} + 24493$	$x^2 + 9x + 16$	20
$10^{1000} + 25947$	$x^2 + 20x + 28$	9
$10^{1000} + 27057$	$(x-9)^2$	18
$10^{1000} + 29737$	$(x-2)(x-1)$	3
$10^{1000} + 41599$	$(x-25)(x-20)$	16
$10^{1000} + 43789$	$(x-9)(x-1)$	10
$10^{1000} + 46227$	$(x-21)(x-4)$	25
$10^{1000} + 46339$	$(x-28)(x-24)$	23
$10^{1000} + 52423$	$x^2 + 27x + 18$	2
$10^{1000} + 55831$	$x^2 + 11x + 4$	18
$10^{1000} + 57867$	$(x-23)(x-19)$	13
$10^{1000} + 59743$	$x^2 + 16x + 27$	13
$10^{1000} + 61053$	$x^2 + 8x + 8$	21
$10^{1000} + 61353$	$(x-24)(x-1)$	25
$10^{1000} + 63729$	$x^2 + 27x + 20$	2
$10^{1000} + 64047$	$(x-25)(x-13)$	9
$10^{1000} + 64749$	$(x-23)(x-5)$	28
$10^{1000} + 68139$	$(x-18)(x-11)$	0
$10^{1000} + 68367$	$(x-24)(x-11)$	6
$10^{1000} + 70897$	$x^2 + 27x + 28$	2
$10^{1000} + 72237$	$(x-28)(x-16)$	15
$10^{1000} + 77611$	$x^2 + 4x + 21$	25
$10^{1000} + 78199$	$(x-21)^2$	13
$10^{1000} + 79237$	$(x-27)(x-2)$	0
$10^{1000} + 79767$	$x^2 + 24x + 16$	5
$10^{1000} + 82767$	$(x-13)(x-2)$	15
$10^{1000} + 93559$	$(x-16)(x-8)$	24
$10^{1000} + 95107$	$x^2 + 7x + 20$	22
$10^{1000} + 100003$	$(x-26)(x-16)$	13

$\ell = 31$

$$f_{12} = \Delta = \sum_{n=1}^{+\infty} \tau(n) q^n = q - 24q^2 + 252q^3 + O(q^4)$$

p	Similarity class of $\left(\frac{L/\mathbb{Q}}{p}\right)$	$\tau(p) \bmod 31$
$10^{1000} + 453$	$(x-30)(x-20)$	19
$10^{1000} + 1357$	$x^2 + 18x + 29$	13
$10^{1000} + 2713$	$x^2 + 27x + 12$	4
$10^{1000} + 4351$	$(x-4)^2$	8
$10^{1000} + 5733$	$(x-21)(x-8)$	29
$10^{1000} + 7383$	$(x-13)(x-11)$	24
$10^{1000} + 10401$	$(x-22)(x-9)$	0
$10^{1000} + 11979$	$(x-7)(x-4)$	11
$10^{1000} + 17557$	$(x-27)^2$	23
$10^{1000} + 21567$	$x^2 + 20x + 27$	11
$10^{1000} + 22273$	$x^2 + 9x + 7$	22
$10^{1000} + 24493$	$x^2 + 27x + 8$	4
$10^{1000} + 25947$	$x^2 + 19x + 25$	12
$10^{1000} + 27057$	$x^2 + 8x + 30$	23
$10^{1000} + 29737$	$(x-17)(x-2)$	19
$10^{1000} + 41599$	$x^2 + x + 2$	30
$10^{1000} + 43789$	$(x-12)(x-4)$	16
$10^{1000} + 46227$	$(x-13)(x-9)$	22
$10^{1000} + 46339$	$x^2 + 28x + 30$	3
$10^{1000} + 52423$	$(x-24)(x-6)$	30
$10^{1000} + 55831$	$(x-30)(x-6)$	5
$10^{1000} + 57867$	$(x-23)(x-7)$	30
$10^{1000} + 59743$	$(x-26)(x-20)$	15
$10^{1000} + 61053$	$x^2 + 10x + 10$	21
$10^{1000} + 61353$	$(x-30)(x-17)$	16
$10^{1000} + 63729$	$(x-20)(x-3)$	23
$10^{1000} + 64047$	$x^2 + 2x + 26$	29
$10^{1000} + 64749$	$x^2 + 13x + 6$	18
$10^{1000} + 68139$	$x^2 + 21x + 26$	10
$10^{1000} + 68367$	$x^2 + 22x + 22$	9
$10^{1000} + 70897$	$x^2 + 8x + 25$	23
$10^{1000} + 72237$	$(x-29)(x-5)$	3
$10^{1000} + 77611$	$x^2 + 20x + 23$	11
$10^{1000} + 78199$	$x^2 + 24x + 17$	7
$10^{1000} + 79237$	$(x-21)(x-16)$	6
$10^{1000} + 79767$	$(x-21)(x-11)$	1
$10^{1000} + 82767$	$(x-8)^2$	16
$10^{1000} + 93559$	$x^2 + 8x + 26$	23
$10^{1000} + 95107$	$x^2 + 9x + 4$	22
$10^{1000} + 100003$	$x^2 + 30x + 2$	1

$$f_{18} = E_6\Delta = \sum_{n=1}^{+\infty} \tau_{18}(n)q^n = q - 528q^2 - 4284q^3 + O(q^4)$$

p	Similarity class of $\left(\frac{L/\mathbb{Q}}{p}\right)$	$\tau_{18}(p)$ mod 31
$10^{1000} + 453$	$x^2 + 10x + 13$	21
$10^{1000} + 1357$	$(x - 25)(x - 11)$	5
$10^{1000} + 2713$	$x^2 + x + 24$	30
$10^{1000} + 4351$	$(x - 20)(x - 19)$	8
$10^{1000} + 5733$	$x^2 + 17x + 22$	14
$10^{1000} + 7383$	$x^2 + 24x + 7$	7
$10^{1000} + 10401$	$x^2 + 24x + 24$	7
$10^{1000} + 11979$	$(x - 13)^2$	26
$10^{1000} + 17557$	$(x - 22)(x - 6)$	28
$10^{1000} + 21567$	$(x - 5)(x - 3)$	8
$10^{1000} + 22273$	$x^2 + 5x + 28$	26
$10^{1000} + 24493$	$(x - 22)(x - 17)$	8
$10^{1000} + 25947$	$x^2 + 25x + 25$	6
$10^{1000} + 27057$	$(x - 19)(x - 13)$	1
$10^{1000} + 29737$	$x^2 + 29x + 17$	2
$10^{1000} + 41599$	$(x - 7)(x - 5)$	12
$10^{1000} + 43789$	$x^2 + 10x + 12$	21
$10^{1000} + 46227$	$(x - 22)(x - 10)$	1
$10^{1000} + 46339$	$x^2 + 8x + 30$	23
$10^{1000} + 52423$	$(x - 17)(x - 12)$	29
$10^{1000} + 55831$	$x^2 + 9x + 25$	22
$10^{1000} + 57867$	$x^2 + 25x + 6$	6
$10^{1000} + 59743$	$(x - 26)(x - 18)$	13
$10^{1000} + 61053$	$x^2 + 23x + 20$	8
$10^{1000} + 61353$	$(x - 16)(x - 7)$	23
$10^{1000} + 63729$	$x^2 + 21x + 27$	10
$10^{1000} + 64047$	$x^2 + 20x + 26$	11
$10^{1000} + 64749$	$(x - 11)(x - 9)$	20
$10^{1000} + 68139$	$(x - 30)(x - 5)$	4
$10^{1000} + 68367$	$(x - 20)(x - 15)$	4
$10^{1000} + 70897$	$(x - 30)(x - 6)$	5
$10^{1000} + 72237$	$(x - 15)(x - 9)$	24
$10^{1000} + 77611$	$(x - 17)(x - 9)$	26
$10^{1000} + 78199$	$(x - 17)(x - 8)$	25
$10^{1000} + 79237$	$(x - 27)(x - 9)$	5
$10^{1000} + 79767$	$x^2 + 2x + 19$	29
$10^{1000} + 82767$	$(x - 18)(x - 14)$	1
$10^{1000} + 93559$	$(x - 15)(x - 10)$	25
$10^{1000} + 95107$	$(x - 8)(x - 2)$	10
$10^{1000} + 100003$	$(x - 2)^2$	4

$$f_{20} = E_8\Delta = \sum_{n=1}^{+\infty} \tau_{20}(n)q^n = q + 456q^2 + 50652q^3 + O(q^4)$$

p	Similarity class of $\left(\frac{L/\mathbb{Q}}{p}\right)$	$\tau_{20}(p)$ mod 31
$10^{1000} + 453$	$(x-21)(x-20)$	10
$10^{1000} + 1357$	$x^2 + 29x + 15$	2
$10^{1000} + 2713$	$(x-25)(x-3)$	28
$10^{1000} + 4351$	$x^2 + x + 2$	30
$10^{1000} + 5733$	$x^2 + 21x + 12$	10
$10^{1000} + 7383$	$x^2 + 30x + 18$	1
$10^{1000} + 10401$	$x^2 + 10x + 13$	21
$10^{1000} + 11979$	$(x-5)(x-2)$	7
$10^{1000} + 17557$	$(x-23)^2$	15
$10^{1000} + 21567$	$(x-16)(x-15)$	0
$10^{1000} + 22273$	$(x-8)(x-5)$	13
$10^{1000} + 24493$	$(x-28)(x-9)$	6
$10^{1000} + 25947$	$(x-9)(x-4)$	13
$10^{1000} + 27057$	$(x-6)(x-5)$	11
$10^{1000} + 29737$	$x^2 + 16x + 21$	15
$10^{1000} + 41599$	$(x-27)^2$	23
$10^{1000} + 43789$	$x^2 + 6x + 11$	25
$10^{1000} + 46227$	$x^2 + 21x + 22$	10
$10^{1000} + 46339$	$x^2 + 24x + 30$	7
$10^{1000} + 52423$	$x^2 + 12x + 14$	19
$10^{1000} + 55831$	$x^2 + 7x + 5$	24
$10^{1000} + 57867$	$(x-28)(x-12)$	9
$10^{1000} + 59743$	$(x-29)(x-20)$	18
$10^{1000} + 61053$	$x^2 + 26x + 28$	5
$10^{1000} + 61353$	$(x-29)(x-21)$	19
$10^{1000} + 63729$	$x^2 + 29x + 15$	2
$10^{1000} + 64047$	$x^2 + 16x + 6$	15
$10^{1000} + 64749$	$(x-23)(x-20)$	12
$10^{1000} + 68139$	$(x-11)(x-9)$	20
$10^{1000} + 68367$	$x^2 + 24x + 24$	7
$10^{1000} + 70897$	$x^2 + 7x + 5$	24
$10^{1000} + 72237$	$(x-16)(x-6)$	22
$10^{1000} + 77611$	$x^2 + x + 27$	30
$10^{1000} + 78199$	$x^2 + 16x + 11$	15
$10^{1000} + 79237$	$(x-17)(x-4)$	21
$10^{1000} + 79767$	$x^2 + 23x + 20$	8
$10^{1000} + 82767$	$(x-25)(x-18)$	12
$10^{1000} + 93559$	$x^2 + 18x + 6$	13
$10^{1000} + 95107$	$x^2 + 26x + 8$	5
$10^{1000} + 100003$	$x^2 + 9x + 16$	22

$$f_{22} = E_{10}\Delta = \sum_{n=1}^{+\infty} \tau_{22}(n)q^n = q - 288q^2 - 128844q^3 + O(q^4)$$

p	Similarity class of $\left(\frac{L/\mathbb{Q}}{p}\right)$	$\tau_{22}(p) \bmod 31$
$10^{1000} + 453$	$(x-27)(x-1)$	28
$10^{1000} + 1357$	$(x-30)(x-2)$	1
$10^{1000} + 2713$	$x^2 + 4x + 29$	27
$10^{1000} + 4351$	$(x-22)(x-12)$	3
$10^{1000} + 5733$	$x^2 + 28x + 15$	3
$10^{1000} + 7383$	$x^2 + 12x + 2$	19
$10^{1000} + 10401$	$(x-22)(x-14)$	5
$10^{1000} + 11979$	$x^2 + 13x + 16$	18
$10^{1000} + 17557$	$x^2 + 6x + 16$	25
$10^{1000} + 21567$	$(x-27)(x-1)$	28
$10^{1000} + 22273$	$(x-21)(x-12)$	2
$10^{1000} + 24493$	$(x-22)(x-6)$	28
$10^{1000} + 25947$	$x^2 + 23x + 1$	8
$10^{1000} + 27057$	$(x-20)(x-17)$	6
$10^{1000} + 29737$	$(x-11)(x-7)$	18
$10^{1000} + 41599$	$(x-18)(x-7)$	25
$10^{1000} + 43789$	$(x-17)(x-5)$	22
$10^{1000} + 46227$	$x^2 + 16x + 27$	15
$10^{1000} + 46339$	$(x-14)(x-11)$	25
$10^{1000} + 52423$	$x^2 + 15x + 4$	16
$10^{1000} + 55831$	$x^2 + 22x + 1$	9
$10^{1000} + 57867$	$(x-20)(x-17)$	6
$10^{1000} + 59743$	$x^2 + 25x + 27$	6
$10^{1000} + 61053$	$(x-2)(x-1)$	3
$10^{1000} + 61353$	$(x-16)^2$	1
$10^{1000} + 63729$	$x^2 + 6x + 29$	25
$10^{1000} + 64047$	$(x-24)(x-9)$	2
$10^{1000} + 64749$	$x^2 + 5x + 30$	26
$10^{1000} + 68139$	$(x-29)(x-16)$	14
$10^{1000} + 68367$	$x^2 + 12x + 23$	19
$10^{1000} + 70897$	$(x-13)(x-12)$	25
$10^{1000} + 72237$	$(x-10)(x-6)$	16
$10^{1000} + 77611$	$(x-17)(x-5)$	22
$10^{1000} + 78199$	$x^2 + 17x + 23$	14
$10^{1000} + 79237$	$(x-18)(x-12)$	30
$10^{1000} + 79767$	$(x-25)(x-9)$	3
$10^{1000} + 82767$	$(x-18)(x-7)$	25
$10^{1000} + 93559$	$x^2 + 7x + 30$	24
$10^{1000} + 95107$	$x^2 + 3x + 4$	28

$$f_{24} = \sum_{n=1}^{+\infty} \tau_{24}(n) q^n = q + 24(22+\alpha)q^2 + 36(4731 - 32\alpha)q^3 + O(q^4)$$

Here we use slightly different notations: f_{24} is the newform of level 1 and of lowest weight to have irrational coefficients, that is to say for which $K_f \neq \mathbb{Q}$. Indeed in this case $K_{f_{24}} = \mathbb{Q}(\sqrt{144169})$ is the quadratic field with integer ring $\mathbb{Z}_{K_{f_{24}}} = \mathbb{Z}[\alpha]$, $\alpha = \frac{1+\sqrt{144169}}{2}$, and (prime) discriminant 144169. The prime 29 is inert in this field, so we could not compute the representation modulo 29 attached to this form; on the contrary, the prime 31 splits into $(31) = \mathfrak{l}_5\mathfrak{l}_{27}$, where $\mathfrak{l}_5 = (31, \alpha - 5)$ and $\mathfrak{l}_{27} = (31, \alpha - 27)$. Instead of presenting the results for the Galois representations attached to f_{24} modulo $\mathfrak{l}_5$ and $\mathfrak{l}_{27}$ separately, it is more interesting to present them together, since we can then compute the coefficients $\tau_{24}(p)$ mod $31\mathbb{Z}[\alpha]$ by putting together the information coming from both representations and using Chinese remainders. This is what we do in the table below, where we denote by L_5 (resp. L_{27}) the number field cut off by the representation modulo $\mathfrak{l}_5$ (resp. $\mathfrak{l}_{27}$) attached to f_{24}.

$$f_{24} = \sum_{n=1}^{+\infty} \tau_{24}(n) q^n = q + 24(22+\alpha)q^2 + 36(4731-32\alpha)q^3 + O(q^4), \quad \alpha = \frac{1+\sqrt{144169}}{2}$$

p	Similarity class of $\left(\frac{L_5/\mathbb{Q}}{p}\right)$	Similarity class of $\left(\frac{L_{27}/\mathbb{Q}}{p}\right)$	$\tau_{24}(p) \bmod 31\mathbb{Z}[\alpha]$
$10^{1000}+453$	$x^2+26x+21$	$(x-20)(x-15)$	$1+7\alpha$
$10^{1000}+1357$	$(x-18)(x-3)$	$(x-25)(x-22)$	$1+4\alpha$
$10^{1000}+2713$	$(x-24)(x-2)$	$(x-29)(x-7)$	$4+23\alpha$
$10^{1000}+4351$	$(x-17)(x-13)$	$(x-11)(x-6)$	$9+29\alpha$
$10^{1000}+5733$	$(x-19)(x-12)$	$(x-15)(x-9)$	$3+18\alpha$
$10^{1000}+7383$	$x^2+4x+14$	$(x-7)(x-2)$	$17+2\alpha$
$10^{1000}+10401$	$(x-22)(x-5)$	$x^2+24x+17$	$9+16\alpha$
$10^{1000}+11979$	$x^2+17x+7$	$x^2+19x+7$	$6+14\alpha$
$10^{1000}+17557$	$(x-26)(x-24)$	$(x-17)(x-13)$	$1+16\alpha$
$10^{1000}+21567$	$x^2+6x+29$	$x^2+2x+29$	$10+3\alpha$
$10^{1000}+22273$	$x^2+10x+19$	$(x-16)(x-7)$	$29+17\alpha$
$10^{1000}+24493$	$(x-22)(x-12)$	$(x-25)(x-18)$	$8+30\alpha$
$10^{1000}+25947$	$(x-15)(x-12)$	$(x-24)(x-23)$	$14+15\alpha$
$10^{1000}+27057$	$x^2+10x+30$	$(x-26)(x-25)$	$17+7\alpha$
$10^{1000}+29737$	$x^2+3x+24$	$x^2+13x+24$	$19+8\alpha$
$10^{1000}+41599$	$x^2+11x+8$	$x^2+27x+8$	$18+19\alpha$
$10^{1000}+43789$	$x^2+14x+3$	x^2+7x+3	$14+13\alpha$
$10^{1000}+46227$	$x^2+15x+12$	$x^2+4x+12$	$29+16\alpha$
$10^{1000}+46339$	$(x-24)(x-9)$	$x^2+5x+30$	$5+18\alpha$
$10^{1000}+52423$	$(x-10)(x-1)$	$x^2+16x+10$	$27+3\alpha$
$10^{1000}+55831$	$x^2+7x+25$	$(x-28)(x-2)$	$17+20\alpha$
$10^{1000}+57867$	$x^2+12x+6$	x^2+6x+6	$12+20\alpha$
$10^{1000}+59743$	$x^2+16x+12$	$(x-21)(x-5)$	$28+16\alpha$
$10^{1000}+61053$	$(x-18)(x-16)$	$x^2+15x+9$	$24+2\alpha$
$10^{1000}+61353$	$(x-26)(x-13)$	$x^2+30x+28$	$11+18\alpha$
$10^{1000}+63729$	$x^2+4x+23$	$(x-18)(x-3)$	$3+11\alpha$
$10^{1000}+64047$	$(x-19)(x-3)$	$(x-13)(x-2)$	$25+18\alpha$
$10^{1000}+64749$	$(x-13)(x-10)$	$(x-17)(x-4)$	$15+14\alpha$
$10^{1000}+68139$	$x^2+2x+26$	$(x-19)(x-3)$	$1+18\alpha$
$10^{1000}+68367$	$(x-22)(x-2)$	$x^2+21x+13$	$30+5\alpha$
$10^{1000}+70897$	$x^2+8x+25$	$(x-26)^2$	$15+14\alpha$
$10^{1000}+72237$	$(x-11)(x-2)$	$(x-12)(x-7)$	$6+20\alpha$
$10^{1000}+77611$	$x^2+5x+15$	$x^2+28x+15$	$27+6\alpha$
$10^{1000}+78199$	$(x-30)(x-28)$	$(x-25)(x-15)$	$17+2\alpha$
$10^{1000}+79237$	$x^2+10x+26$	$(x-27)(x-9)$	$19+19\alpha$
$10^{1000}+79767$	$(x-15)(x-6)$	$(x-7)(x-4)$	$12+8\alpha$
$10^{1000}+82767$	$(x-13)(x-3)$	$(x-24)(x-21)$	$8+14\alpha$
$10^{1000}+93559$	$(x-15)(x-10)$	$x^2+8x+26$	$17+14\alpha$
$10^{1000}+95107$	$(x-28)(x-20)$	$(x-18)(x-7)$	$18+6\alpha$
$10^{1000}+100003$	$x^2+21x+8$	$(x-10)(x-7)$	$7+13\alpha$

$$f_{26} = E_{14}\Delta = \sum_{n=1}^{+\infty} \tau_{26}(n)q^n = q - 48q^2 - 195804q^3 + O(q^4)$$

p	Similarity class of $\left(\frac{L/\mathbb{Q}}{p}\right)$	$\tau_{26}(p)$ mod 31
$10^{1000} + 453$	$(x-3)(x-2)$	5
$10^{1000} + 1357$	$(x-23)(x-4)$	27
$10^{1000} + 2713$	$x^2 + 13x + 26$	18
$10^{1000} + 4351$	$(x-13)(x-12)$	25
$10^{1000} + 5733$	$(x-6)(x-1)$	7
$10^{1000} + 7383$	$x^2 + 27x + 5$	4
$10^{1000} + 10401$	$x^2 + 21x + 26$	10
$10^{1000} + 11979$	$(x-27)(x-22)$	18
$10^{1000} + 17557$	$(x-17)(x-11)$	28
$10^{1000} + 21567$	$(x-27)(x-8)$	4
$10^{1000} + 22273$	$x^2 + 2x + 5$	29
$10^{1000} + 24493$	$(x-9)(x-7)$	16
$10^{1000} + 25947$	$(x-20)(x-8)$	28
$10^{1000} + 27057$	$(x-18)(x-12)$	30
$10^{1000} + 29737$	$(x-25)(x-6)$	0
$10^{1000} + 41599$	$x^2 + 23x + 1$	8
$10^{1000} + 43789$	$x^2 + 8x + 26$	23
$10^{1000} + 46227$	$x^2 + 10x + 26$	21
$10^{1000} + 46339$	$x^2 + 22x + 30$	9
$10^{1000} + 52423$	$(x-22)(x-11)$	2
$10^{1000} + 55831$	$x^2 + 17x + 5$	14
$10^{1000} + 57867$	$(x-28)(x-12)$	9
$10^{1000} + 59743$	$x^2 + x + 26$	30
$10^{1000} + 61053$	$(x-5)^2$	10
$10^{1000} + 61353$	$x^2 + 2x + 5$	29
$10^{1000} + 63729$	$(x-29)(x-16)$	14
$10^{1000} + 64047$	$(x-3)(x-2)$	5
$10^{1000} + 64749$	$(x-29)(x-18)$	16
$10^{1000} + 68139$	$x^2 + 27x + 6$	4
$10^{1000} + 68367$	$(x-6)(x-1)$	7
$10^{1000} + 70897$	$x^2 + 24x + 5$	7
$10^{1000} + 72237$	$(x-23)(x-7)$	30
$10^{1000} + 77611$	$x^2 + 8x + 30$	23
$10^{1000} + 78199$	$(x-30)(x-5)$	4
$10^{1000} + 79237$	$(x-11)(x-9)$	20
$10^{1000} + 79767$	$x^2 + 24x + 5$	7
$10^{1000} + 82767$	$x^2 + 20x + 1$	11
$10^{1000} + 93559$	$x^2 + 19x + 6$	12
$10^{1000} + 95107$	$(x-29)(x-15)$	13
$10^{1000} + 100003$	$(x-19)(x-18)$	6

4 Certifying the polynomials

The results presented above rely on the identification by continued fractions of rational numbers given in approximate form as floating-point numbers. In order to certify these results, it is thus necessary to make sure that the number fields cut out by the representations as well as the Galois action on them have been correctly identified.

For this, a first possibility consists in proving bounds on the height of the rational numbers which the algorithm will have to identify, and then to certify that the continued fraction identification process is correct, for instance by running the computation with high enough precision in $\mathbb{C}$ and controlling the round-off errors all along. Although it is indeed possible to bound the height of these rational numbers by using Arakelov theory (cf. [CE11, theorem 11.7.6]), this approach gives unrealistic titanic bounds and thus seems ominously tedious, especially as it requires controlling the round-off error in the linear algebra steps K. Khuri-Makdisi's algorithms to compute in the modular Jacobian (cf. [Mas13, section 3.3]). We have therefore not attempted to follow it. Instead, we deemed it much better to first run the computations in order to obtain unproven results, and to prove these results afterwards.

We explain in this section how this to prove formally that the number field cut out by the Galois representation $\rho_{f,\mathfrak{l}}$ has been correctly identified, in the case of a newform f of level $N = 1$. Unfortunately, we do not know at present how to efficiently prove formally that the Galois action on the roots of the polynomials computed by the algorithm is the expected one, so that we cannot formally prove that the values of the coefficients $a_p \bmod \mathfrak{l}$ are correct either.

4.1 Sanity checks

Before attempting to prove the results, it is comforting to perform a few easy checks so as to ensure that these results seem correct beyond reasonable doubt (cf the end of section 1 in [Mas13]). Namely,

- Since we are working with a form of level $N = 1$, the number field L cut out by the Galois representation $\rho_{f,\mathfrak{l}}$ is ramified only at ℓ. Therefore, we can check that the discriminant of the polynomial $F(X) \in \mathbb{Q}[X]$ is of the form

$$\pm \ell^n M^2$$

  for some $M \in \mathbb{Q}^*$. Better,we can compute the maximal order of the field $K = \mathbb{Q}[X]/F(X)$ whose Galois closure is L and check that its discriminant is, up to sign, a power of ℓ. Since a number field ramifies at the same primes as its Galois closure, this proves that the decomposition field L of $F(X)$ is ramified only at ℓ, as expected.

- Since Galois representations attached to modular forms are odd, the image of complex conjugation by these representations is an involutive matrix in $\mathrm{GL}_2(\mathbb{F}_\mathfrak{l})$ of determinant -1, hence similar to $\left[\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right]$ if $\ell \geqslant 2$. This means that the polynomial $F(X)$ of degree $\ell^2 - 1$ computed by the algorithm should have exactly $\ell - 1$ roots in $\mathbb{R}$, which can be checked numerically, and that the sign of its discriminant should be $(-1)^{\ell(\ell-1)/2}$, which can be checked exactly.

- The fact that the resolvents $\Gamma_C(X)$ computed by the Dokchitsers' method and used to identify the image of Frobenius elements seem to have integer (and not just complex) coefficients hints that $\mathrm{Gal}(L/\mathbb{Q})$ is indeed isomorphic to a subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$, so that the number field L is indeed a number field cut out by a Galois representation, and that the Galois action on $V_{f,\mathfrak{l}} \subset J_1(\ell)[\ell]$ is linear.

- The fact that the polynomials $F^S(X)$ computed by regrouping the roots of $F(X)$ along their S-orbits for the various subgroups $S \subseteq \mathbb{F}_\ell^*$ considered during the polynomial reduction process (cf. section 2) seem to have rational coefficients with common denominator dividing the one of $F(X)$ also hints that the coefficients of these polynomials have been correctly identified as rational numbers, that $\mathrm{Gal}(L/\mathbb{Q})$ is indeed isomorphic to a subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$, and that the Galois action on the root of $F(X)$ is the expected one.

- Finally, we can check that the values $a_p \bmod \mathfrak{l}$ obtained by the algorithm for a few small primes p are correct, by comparing them with the ones computed by "classical" methods such as based on modular symbol-based ones.

4.2 Proving the polynomials

We shall now present a method to formally prove that the splitting fields the polynomials computed by the algorithm are the number fields cut out by the corresponding Galois representations. This method proceeds from the bottom up, in that it consists in first proving the correctness of the projective Galois representation $\rho_{f,\mathfrak{l}}^{\mathrm{proj}}$, then the correctness of the quotient Galois representation $\rho_{f,\mathfrak{l}}^S$ where S is gradually refined from the whole of $\mathbb{F}_\mathfrak{l}^*$ to the maximal subgroup of $\mathbb{F}_\mathfrak{l}^*$ not containing -1. In each case, we first prove that we are indeed dealing with a Galois representation of the correct kind, which amounts to proving that the Galois group of the polynomial computed by the algorithm is the correct one, and then we prove that the splitting field of this polynomial is the correct one, that is to say the number field cut out by the appropriate quotient $\rho_{f,\mathfrak{l}}^S$ of $\rho_{f,\mathfrak{l}}$.

We shall assume that it has been checked that the polynomials $F^{\mathrm{proj}}(X)$ and $F^S(X)$ computed by the algorithm and reduced as in section 2 are irreducible over $\mathbb{Q}$.

4.2.1 Proving the projective representation

We begin with the projective Galois representation $\rho_{f,\mathfrak{l}}^{\mathrm{proj}}$, which ought to be defined by the monic polynomial $F^{\mathrm{proj}}(X) \in \mathbb{Z}[X]$ of degree $\ell + 1$ obtained by the `polred` algorithm (cf. section 2). We denote the splitting field of $F^{\mathrm{proj}}(X)$ in $\mathbb{C}$ by L^{proj}.

Proving the Galois group

The first thing to do is to make sure that this polynomial does define a projective Galois representation, by proving that $\mathrm{Gal}(L^{\mathrm{proj}}/\mathbb{Q})$ is isomorphic to a subgroup of $\mathrm{PGL}_2(\mathbb{F}_\ell)$. Since we are dealing with an non-exceptional case, in the sense that the image of the linear representation $\rho_{f,\mathfrak{l}}$ should contain $\mathrm{SL}_2(\mathbb{F}_\ell)$, this subgroup should be either $\mathrm{PGL}_2(\mathbb{F}_\ell)$ or $\mathrm{PSL}_2(\mathbb{F}_\ell)$; and since we are dealing with forms of level $N = 1$, hence of trivial nebentypus ε, and of even weight, the determinant of $\rho_{f,\mathfrak{l}}$ is an odd

power of the mod ℓ cyclotomic character, and so there are matrices with non-square determinant in its image, so that $\mathrm{Gal}(L^{\mathrm{proj}}/\mathbb{Q})$ should actually be isomorphic to the whole of $\mathrm{PGL}_2(\mathbb{F}_\ell)$.

The roots a_x, $x \in \mathbb{P}^1\mathbb{F}_\ell$ of $F^{\mathrm{proj}}(X)$ in $\mathbb{C}$ computed by the algorithm are by construction indexed by $\mathbb{P}^1\mathbb{F}_\ell$. Consider the resolvent polynomial

$$R_4^{\mathrm{proj}}(X) = \prod_{\substack{x_1,x_2,x_3,x_4 \in \mathbb{P}^1\mathbb{F}_\ell \\ \text{pairwise distinct}}} \big(X - (\lambda_1 a_{x_1} + \lambda_2 a_{x_2} + \lambda_3 a_{x_3} + \lambda_4 a_{x_4})\big) \in \mathbb{Z}[X]$$

which monitors the Galois action on ordered quadruplets of roots of $F^{\mathrm{proj}}(X)$, where $\lambda_1, \cdots, \lambda_4 \in \mathbb{Z}$ are fixed integer parameters chosen so that $R_4^{\mathrm{proj}}(X)$ is squarefree.

In order to compute this resolvent formally, we express it in terms of *composed sums*. recall that the composed sum of two polynomials f and $g \in \mathbb{Q}[X]$ is

$$f \oplus g = \prod_{f(\alpha)=g(\beta)=0} \big(X - (\alpha + \beta)\big),$$

where the product runs over the roots α of f and β of g in $\overline{\mathbb{Q}}$ counted with multiplicity. As explained in [BFSS06], composed sums can be computed with quasilinear complexity as follows:

Define, for monic $f \in \mathbb{Q}[X]$, the *exponential Newton sum generating series* of f by

$$H(f) = \sum_{n=0}^{+\infty} \frac{\nu_n(f)}{n!} T^n \in \mathbb{Q}\big[[T]\big],$$

where the $\nu_n(f)$ are the *Newton sums* of f,

$$\nu_n(f) = \sum_{f(\alpha)=0} \alpha^n,$$

the sum running over the roots α of f in $\overline{\mathbb{Q}}$ counted with multiplicity. Then for $B \geqslant \deg f$, the conversion between f and $H(f) \bmod T^B$ can be performed in $\widetilde{O}(B)$ bit operations, by using fast power series arithmetic and the formulae

$$\sum_{n=0}^{\infty} \nu_n(f) T^n = \sum_{f(\alpha)=0} \frac{1}{1-\alpha T} = \frac{\mathrm{rev}(f')}{\mathrm{rev}(f)}$$

in the one way, and

$$\mathrm{rev}(f) = \exp\left(-\sum_{n=1}^{\infty} \frac{\nu_n}{n} T^n\right)$$

in the other way, where $\mathrm{rev}(f) = X^{\deg f} f(1/X)$ denotes the reverse of a polynomial f. Since furthermore

$$H(f \oplus g) = H(f)H(g)$$

for any two polynomials f and g in $\mathbb{Q}[X]$, this yields a quasilinear method to symbolically compute composed sums, and hence the resolvent $R_4^{\mathrm{proj}}(X)$.

Once we have computed the resolvent $R_4^{\mathrm{proj}}(X)$ symbolically and ensured that it is squarefree, we compute numerically a complex approximation of the factor

$$R_x(X) = \prod_{\substack{x_1,x_2,x_3,x_4 \in \mathbb{P}^1\mathbb{F}_\ell \\ \text{pairwise distinct} \\ [x_1,x_2,x_3,x_4]=x}} \big(X - (\lambda_1 a_{x_1} + \lambda_2 a_{x_2} + \lambda_3 a_{x_3} + \lambda_4 a_{x_4})\big) \in \mathbb{C}[X]$$

for each $x \in \mathbb{P}^1\mathbb{F}_\ell - \{\infty, 0, 1\}$, where $[x_1, x_2, x_3, x_4] = \frac{x_3-x_1}{x_3-x_2}\frac{x_4-x_2}{x_4-x_1} \in \mathbb{P}^1\mathbb{F}_\ell$ denotes the cross-ratio (a.k.a. anharmonic ratio) of the x_i, and check that this approximation seems to lie in $\mathbb{Z}[X]$. We then check that the polynomials $R_x(X)$ all divide $R_4^{\mathrm{proj}}(X)$ in $\mathbb{Z}[X]$. This proves that the action of $\mathrm{Gal}(L^{\mathrm{proj}}/\mathbb{Q})$ on the ordered quadruplets of roots of $F^{\mathrm{proj}}(X)$ preserves the cross-ratio, which implies that $\mathrm{Gal}(L^{\mathrm{proj}}/\mathbb{Q})$ is a subgroup of $\mathrm{PGL}_2(\mathbb{F}_\ell)$ acting on the roots a_x, $x \in \mathbb{P}^1\mathbb{F}_\ell$ of $F^{\mathrm{proj}}(X)$ in the same way as $\mathrm{PGL}_2(\mathbb{F}_\ell)$ acts on $\mathbb{P}^1\mathbb{F}_\ell$.

Correctness of the projective representation

Now that we have made sure that the Galois action on the roots of $F^{\mathrm{proj}}(X)$ does define a projective representation

$$\rho^{\mathrm{proj}} \colon G_{\mathbb{Q}} \twoheadrightarrow \mathrm{Gal}(L^{\mathrm{proj}}/\mathbb{Q}) \hookrightarrow \mathrm{PGL}_2(\mathbb{F}_\ell)\ ,$$

we prove that this representation is isomorphic to $\rho_{f,\mathfrak{l}}^{\mathrm{proj}}$ as expected. For this, we use the following theorem from [Bos07]:

Theorem 1. *Let $\pi \colon G_{\mathbb{Q}} \longrightarrow \mathrm{PGL}_2(\mathbb{F}_\ell)$ be an projective mod ℓ Galois representation. Let $H \subset \mathrm{PGL}_2(\mathbb{F}_\ell)$ be the stabiliser of a point of $\mathbb{P}^1\mathbb{F}_\ell$, and let $K = \overline{\mathbb{Q}}^{\pi^{-1}(H)}$ be the corresponding number field. If the number field L cut out by π is not totally real and if there exists an integer k such that*

$$\operatorname{disc} K = \pm\ell^{k+\ell-2},$$

then there exists a newform $f \in S_k(1)$ and a prime $\mathfrak{l}$ of $\overline{\mathbb{Q}}$ above ℓ such that

$$\pi \sim \rho_{f,\mathfrak{l}}^{proj}.$$

Sketch. The idea is that the projective representation π can be lifted to a linear representation

$$\rho \colon G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\overline{\mathbb{F}_\ell})$$

which, just like π, is irreducible and ramifies only at ℓ. Furthermore, the image of the complex conjugation (corresponding to some embedding of L into $\mathbb{C}$) by ρ has order at most 2, so is similar to either $\left[\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right]$, $\left[\begin{smallmatrix}-1&0\\0&-1\end{smallmatrix}\right]$ or $\left[\begin{smallmatrix}1&0\\0&-1\end{smallmatrix}\right]$, but the first two are impossible since they reduce to the identity in $\mathrm{PGL}_2(\mathbb{F}_\ell)$ and L is not totally real, which proves that ρ is odd. Serre's modularity conjecture (cf. [KW09]) then applies and shows that ρ is modular, say $\rho \sim \rho_{f,\mathfrak{l}}$ for some newform $f \in S_{k_\rho}(N_\rho, \varepsilon_\rho)$ and some prime $\mathfrak{l}$ of $\overline{\mathbb{Q}}$ above ℓ. Then, since ρ ramifies only at ℓ, its Artin conductor is a power of ℓ, so ρ comes from a form f of level $N_\rho = 1$; in particular, the nebentypus ε_ρ of f is trivial. Finally, if the lift ρ is chosen so that the weight k_ρ of f is minimal, then [MT03, theorem 3] gives a formula for the ℓ-adic valuation of the discriminant of the Galois number field cut out by ρ, which by J. Bosman's work boils down to

$$\operatorname{disc} K = \pm\ell^{k_\rho+\ell-2}.$$

□

Thus, in order to prove that $\rho^{\mathrm{proj}} \sim \rho^{\mathrm{proj}}_{f,\mathfrak{l}}$, all we have to do is check that not all the roots of $F^{\mathrm{proj}}(X)$ are real, which can be done by using Sturm's method (cf. [Lan02, chapter XI, theorem 2.7]), and that the discriminant of the rupture field $K^{\mathrm{proj}} = \mathbb{Q}[X]/F^{\mathrm{proj}}(X)$ is $\pm\ell^{k+\ell-2}$, which is a piece of cake for [Pari/GP].

Except in the case $\ell = 31, k = 24$ (cf. page 29), this concludes in all the cases which I have considered in section 3, since $\dim S_k(1) = 1$ so that there is only one possibility for f, and the coefficients of f are rational so that the choice of the prime $\mathfrak{l}$ lying above ℓ does not matter. In the special case $\ell = 31, k = 24$, we still know that ρ^{proj} is equivalent to either $\rho^{\mathrm{proj}}_{f_{24},\mathfrak{l}_5}$ or its conjugate $\rho^{\mathrm{proj}}_{f_{24},\mathfrak{l}_{27}}$. In order to tell which, we pick a small prime $p \in \mathbb{N}$ which does not divide $\operatorname{disc} F^{\mathrm{proj}}(X)$ (in particular $p \neq \ell$), and such that $\tau_{24}(p) \equiv 0 \bmod \mathfrak{l}_5$ but $\tau_{24}(p) \not\equiv 0 \bmod \mathfrak{l}_{27}$ (the opposite would do too). Since an element of $\mathrm{PGL}_2(\mathbb{F}_\ell)$ is of order 2 if and only if it has trace 0, looking at the factorisation of $F^{\mathrm{proj}}(X) \bmod p$ allows us to tell $\mathfrak{l}_5$ and $\mathfrak{l}_{27}$ apart: if $F^{\mathrm{proj}}(X)$ splits into linear and quadratic factors in $\mathbb{F}_p[X]$, then it is associated to $\rho^{\mathrm{proj}}_{f_{24},\mathfrak{l}_5}$, else it is associated to $\rho^{\mathrm{proj}}_{f_{24},\mathfrak{l}_{27}}$.

In particular, this implies that the Galois group $\mathrm{Gal}(L_0/\mathbb{Q})$ is isomorphic to the whole of $\mathrm{PGL}_2(\mathbb{F}_\ell)$, whereas we had only proved that it was isomorphic to a transitive subgroup thereof until now.

4.2.2 Proof of the polynomial $F^S(X)$

We now explain how to prove the correctness of the polynomial $F^S(X)$ defining the quotient representation. Write $\ell - 1 = 2^r s$ with $s = |S|$ odd, and recall that we considered in section 2 the filtration

$$\mathbb{F}_\ell^* = S_0 \underset{2}{\supset} S_1 \underset{2}{\supset} \cdots \underset{2}{\supset} S_r = S$$

with $[S_i : S_{i+1}] = 2$ for all i, so that

$$S_i = \mathrm{Im}\begin{pmatrix} \mathbb{F}_\ell^* & \longrightarrow & \mathbb{F}_\ell^* \\ x & \longmapsto & x^{2^i} \end{pmatrix},$$

and we computed polynomials $F_i(X) \in \mathbb{Z}[X]$ such that the Galois action on the roots of $F_i(X)$ is supposed to yield the quotient Galois representation

$$\rho^{S_i}_{f,\mathfrak{l}} \colon\ G_{\mathbb{Q}} \xrightarrow{\rho_{f,\mathfrak{l}}} \mathrm{GL}_2(\mathbb{F}_\ell) \twoheadrightarrow \mathrm{GL}_2(\mathbb{F}_\ell)/S_i\ .$$

Let $K_i = \mathbb{Q}[X]/F_i(X)$ be the rupture field of $F_i(X)$, and L_i be its Galois closure, which is thus supposed to be the number field cut out by ρ^{S_i}. We have just proved above that it is so for $i = 0$.

For each $i < r$, the extension K_{i+1}/K_i is quadratic by construction, generated by the square root of some primitive element δ_i of K_i, which we assume to be integral. Let $\ell^* = (-1)^{(\ell-1)/2}\ell$, so that $\mathbb{Q}(\sqrt{\ell^*})$ is the unique quadratic number field which ramifies only at ℓ, and consider the following assertions:

(A1) The polynomials $F_i(X)$ are irreducible in $\mathbb{Q}[X]$, and their decomposition fields L_i ramify only at ℓ.

(A2) For each i, let $\Delta_i(X) \in \mathbb{Z}[X]$ be the monic minimal polynomial of δ_i over $\mathbb{Q}$, and let

$$Q_i(X) = \frac{\mathrm{Res}_Y\left(\Delta_i(Y), \Delta_i(XY)\right)}{(X-1)^{2^i(\ell+1)}} \in \mathbb{Z}[X].$$

Then $Q_i(X)$ is irreducible over $\mathbb{Q}$ and even over $\mathbb{Q}(\sqrt{\ell^*})$, but $Q_i(X^2)$ splits into two factors of equal degrees over $\mathbb{Q}(\sqrt{\ell^*})$.

These assertions can be checked easily with [Pari/GP]. For (A1), it suffices to check that the discriminant of the rupture field K_i of $F_i(X)$ is of the form $\pm\ell^n$ for some $n \in \mathbb{N}$. For (A2), note that if $f = \prod_{i=1}^{n}(X - \alpha_i)$, then

$$\mathrm{Res}_Y\left(\Delta_i(Y), \Delta_i(XY)\right) = (-1)^n f(0) \prod_{i,j} \left(X - \frac{\alpha_i}{\alpha_j}\right),$$

so that

$$\frac{\mathrm{Res}_Y\left(\Delta_i(Y), \Delta_i(XY)\right)}{(X-1)^n} = (-1)^n f(0) \prod_{i \neq j} \left(X - \frac{\alpha_i}{\alpha_j}\right)$$

is indeed a polynomial.

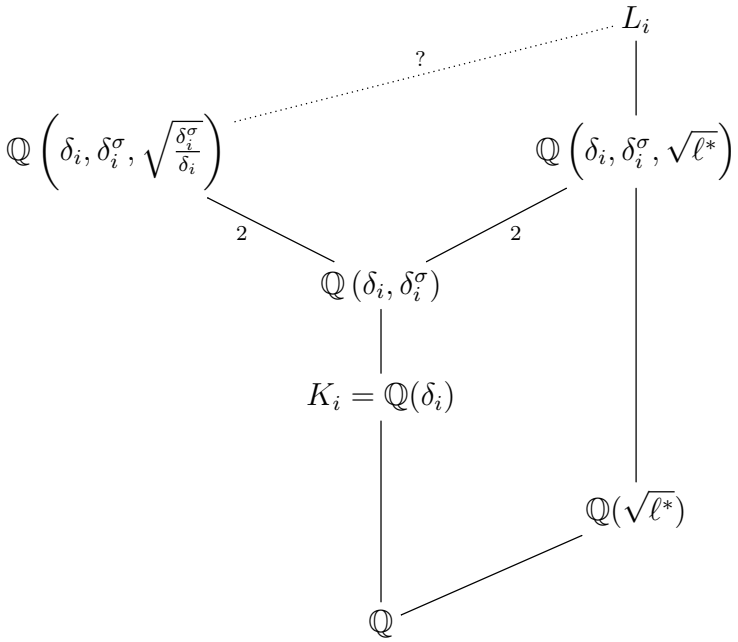
We shall see below that both (A1) and (A2) should hold if the polynomials $F_i(X)$ have been correctly computed by the algorithm. Conversely, we are now going to prove the following result, which thus yields an efficient method to formally prove that the polynomials $F_i(X)$ have been correctly computed:

Theorem 2. *Assume that the assertions (A1) and (A2) hold all $i \leqslant r$. Then for all $i \leqslant r$, L_i is the number field cut out by $\rho_{f,\mathfrak{l}}^{S_i}$.*

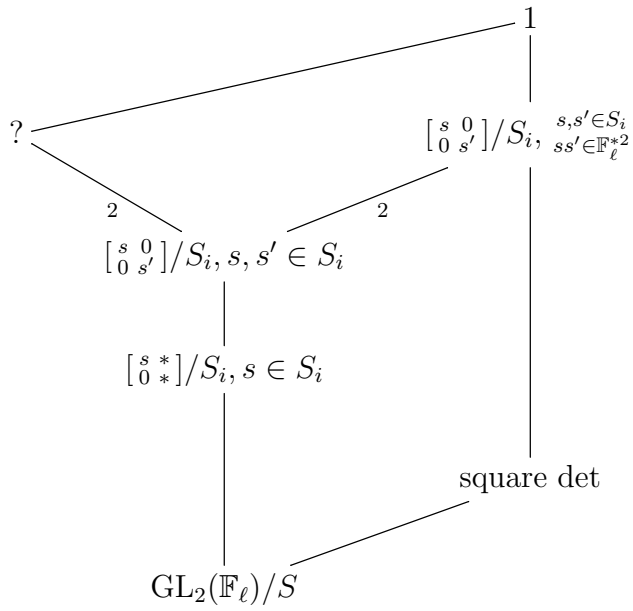
We thus assume henceforth that (A1) and (A2) hold. To begin with, we shall prove that $\mathrm{Gal}(L_i/\mathbb{Q})$ is isomorphic to $\mathrm{GL}_2(\mathbb{F}_\ell)/S_i$ for all i. Since $K_{i+1} = K_i(\sqrt{\delta_i})$, we have

$$L_{i+1} = L_i\big(\sqrt{\delta_i^\sigma}, \sigma \in \mathrm{Gal}(L_i/\mathbb{Q})\big).$$

We first claim that actually $L_{i+1} = L_i(\sqrt{\delta_i})$ is a quadratic extension of L_i, that is to say that $\frac{\delta_i^\sigma}{\delta_i}$ is a square in L_i for all $\sigma \in \mathrm{Gal}(L_i/\mathbb{Q})$. To see this, note that since $\mathrm{PGL}_2(\mathbb{F}_\ell)$ has a quotient $\mathrm{PGL}_2(\mathbb{F}_\ell)/\mathrm{PSL}_2(\mathbb{F}_\ell)$ of order 2, the field $L_i \supset L_0$ has a quadratic subfield, which can only be $\mathbb{Q}(\sqrt{\ell^*})$ since L_i ramifies only at ℓ by (A1). Consider the extension diagram



Assume for now that the extensions marked with a 2 are indeed quadratic and not trivial. If L_i **were** the number field cut out by $\rho_{f,\mathfrak{l}}^{S_i}$, then the corresponding Galois subgroup diagram would be



and since the group

$$\left\{ \begin{bmatrix} s & 0 \\ 0 & s' \end{bmatrix} /S_i,\ s, s' \in S_i \right\} \simeq \mathbb{F}_\ell^*/S_i$$

is cyclic, it has only one subgroup of index 2, so that these two quadratic extensions would agree and (A2) would hence be satisfied.

Now, back to the proof, letting $n = 2^i(\ell+1) = [K_i\colon \mathbb{Q}]$, then

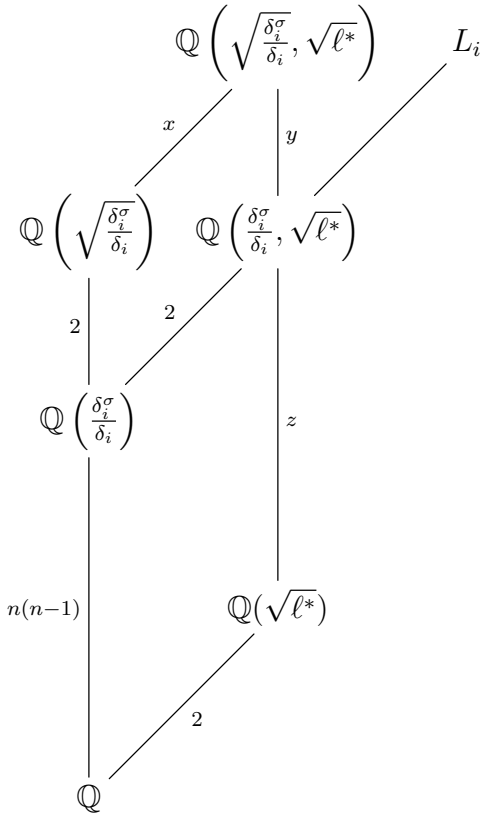
$$[\mathbb{Q}(\delta_i, \delta_i^\sigma) : \mathbb{Q}] = [\mathbb{Q}(\delta_i, \delta_i^\sigma) : \mathbb{Q}(\delta_i)][\mathbb{Q}(\delta_i) : \mathbb{Q}] \leqslant (n-1)n,$$

whereas

$$\left[\mathbb{Q}\left(\frac{\delta_i^\sigma}{\delta_i}\right) : \mathbb{Q}\right] = \deg Q_i(X) = (n-1)n$$

since $Q_i(X)$ is irreducible over $\mathbb{Q}$ by (A2), so that $\mathbb{Q}(\delta_i, \delta_i^\sigma) = \mathbb{Q}\left(\frac{\delta_i^\sigma}{\delta_i}\right)$. Furthermore, the extension $\mathbb{Q}\left(\frac{\delta_i^\sigma}{\delta_i}, \sqrt{\ell^*}\right)/\mathbb{Q}\left(\frac{\delta_i^\sigma}{\delta_i}\right)$ is not trivial since $Q_i(X)$ is irreducible over $\mathbb{Q}(\sqrt{\ell^*})$ by (A2). We may also assume that the extension $\mathbb{Q}\left(\sqrt{\frac{\delta_i^\sigma}{\delta_i}}\right)/\mathbb{Q}\left(\frac{\delta_i^\sigma}{\delta_i}\right)$ is not trivial, since the proof that $\sqrt{\frac{\delta_i^\sigma}{\delta_i}} \in L_i$ is over if it is. The two extensions marked with a 2 in the extension tower above are thus non-trivial, hence quadratic, so that

we have the extension diagram



where the labels denote the degrees. By looking at the bottom parallelogram, we see that $z = n(n-1)$, so that $x = y$ by looking at the top parallelogram. Now since $Q_i(X^2)$ splits into two factors of degrees $n(n-1)$ over $\mathbb{Q}(\sqrt{\ell^*})$ by (A2), we have

$$\left[\mathbb{Q}\left(\sqrt{\frac{\delta_i^\sigma}{\delta_i}}, \sqrt{\ell^*}\right) : \mathbb{Q}(\sqrt{\ell^*})\right] = n(n-1),$$

so that $y = 1$, whence $x = 1$. Therefore

$$\mathbb{Q}\left(\sqrt{\frac{\delta_i^\sigma}{\delta_i}}\right) = \mathbb{Q}\left(\sqrt{\frac{\delta_i^\sigma}{\delta_i}}, \sqrt{\ell^*}\right) = \mathbb{Q}\left(\frac{\delta_i^\sigma}{\delta_i}, \sqrt{\ell^*}\right) \subset L_i,$$

so that $\sqrt{\frac{\delta_i^\sigma}{\delta_i}} \in L_i$ as I claimed.

As a consequence, $L_{i+1} = L_i(\sqrt{\delta_i})$ and $\mathrm{Gal}(L_{i+1}/\mathbb{Q})$ is an extension of $\mathrm{Gal}(L_i/\mathbb{Q})$ by $\mathbb{Z}/2\mathbb{Z}$, which is necessarily central since $\mathrm{Aut}(\mathbb{Z}/2\mathbb{Z})$ is trivial.

Recall now that given a group G and a G-module M, the extensions of G by M such that the conjugation action of lifts of elements of G on M corresponds to the G-module structure on M are classified by the cohomology group $H^2(G, M)$, the class of the cocycle $\beta\colon G \times G \longrightarrow M$ corresponding to the set $M \times G$ endowed with the group law

$$(m, g) \cdot (m', g') = \big(m + g \cdot m' + \beta(g, g'), gg'\big).$$

In particular, the following result is immediate:

Lemma 3. *Consider a (necessarily central) extension*

$$0 \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow \widetilde{G} \longrightarrow G \longrightarrow 1$$

of a group G by $\mathbb{Z}/2\mathbb{Z}$. Let $\beta\colon G \times G \longrightarrow \mathbb{Z}/2\mathbb{Z}$ be a cocycle representing the corresponding cohomology class, and let $g \in G$ be an element of G of order 2. Then the lifts of g in $\widetilde{G}$ have order 2 if $\beta(g, g) = 0$, but have order 4 if $\beta(g, g) = 1$.

Furthermore (cf. [Kar87, theorem 2.1.19]), if M is a trivial G-module, there is a split exact sequence of abelian groups

$$0 \longrightarrow \mathrm{Ext}^1_{\mathbb{Z}}(G^{\mathrm{ab}}, M) \overset{\phi}{\hookrightarrow} H^2(G, M) \underset{\iota}{\overset{\psi}{\rightleftarrows}} \mathrm{Hom}\left(\widehat{M}, H^2(G, \mathbb{C}^*)\right) \longrightarrow 0 \qquad (\star)$$

where $\mathrm{Ext}^1_{\mathbb{Z}}(G^{\mathrm{ab}}, M)$ classifies the abelian extensions of the abelianised G^{ab} of G by M, $\widehat{M} = \mathrm{Hom}(M, \mathbb{C}^*)$ is the group of complex-valued characters on M, $H^2(G, \mathbb{C}^*)$ (with trivial G-action on $\mathbb{C}^*$) is the so-called *Schur multiplier* of G, and ψ maps the class of the cocycle $\beta \in H^2(G, M)$ to the *transgression map* (not to be confused with a trace)

$$\begin{array}{rccc} \mathrm{Tra}_\beta\colon & \widehat{M} & \longrightarrow & H^2(G, \mathbb{C}^*) \\ & \chi & \longmapsto & \chi \circ \beta \end{array}$$

associated to the class of β. Besides, the Schur multiplier $H^2(G, \mathbb{C}^*)$ is trivial if G is cyclic (cf. [Kar87, proposition 2.1.1.(ii)]), and for each central extension $\widetilde{G}$ of G by M, the subgroup $M \cap D\widetilde{G}$ of $\widetilde{G}$ is isomorphic to the image of Tra_β, where $\beta \in H^2(G, M)$ is the cohomology class corresponding to $\widetilde{G}$, and $D\widetilde{G}$ denotes the commutator subgroup of $\widetilde{G}$ (cf. [Kar87, proposition 2.1.7]).

Applying this to the group $G = \mathrm{PGL}_2(\mathbb{F}_\ell)$ and the trivial G-module $M = \mathbb{Z}/2^i\mathbb{Z}$ yields the following result (cf. [Que95]):

Theorem 4. *Let $i \in \mathbb{N}$.*

(i) $H^2\big(\mathrm{PGL}_2(\mathbb{F}_\ell), \mathbb{Z}/2^i\mathbb{Z}\big) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$*, so that there are four central extensions of* $\mathrm{PGL}_2(\mathbb{F}_\ell)$ *by* $\mathbb{Z}/2^i\mathbb{Z}$*.*

(ii) These extensions are

- *the trivial extension* $\mathbb{Z}/2^i\mathbb{Z} \times \mathrm{PGL}_2(\mathbb{F}_\ell)$*, corresponding to the trivial cohomology class* $\beta_0 \in H^2\big(\mathrm{PGL}_2(\mathbb{F}_\ell), \mathbb{Z}/2^i\mathbb{Z}\big)$*,*
- *the group* $2^i_{\det}\mathrm{PGL}_2(\mathbb{F}_\ell)$*, whose associated cohomology class* $\beta_{\det} \in H^2\big(\mathrm{PGL}_2(\mathbb{F}_\ell), \mathbb{Z}/2^i\mathbb{Z}\big)$ *is the inflation of the non-trivial element of*

$$H^2\big(\mathrm{PGL}_2(\mathbb{F}_\ell)^{\mathrm{ab}}, \mathbb{Z}/2^i\mathbb{Z}\big) \simeq \mathbb{Z}/2\mathbb{Z}$$

  (in other words, $\beta_{\det}(g, g')$ *is non-zero if and only if neither* g *nor* g' *lie in* $\mathrm{PSL}_2(\mathbb{F}_\ell)$*),*

- *the group* $2^i_-\mathrm{PGL}_2(\mathbb{F}_\ell)$*, with associated cohomology class* $\beta_- \in H^2\big(\mathrm{PGL}_2(\mathbb{F}_\ell), \mathbb{Z}/2^i\mathbb{Z}\big)$*, defined for* $i = 1$ *as*

$$2_-\mathrm{PGL}_2(\mathbb{F}_\ell) = \mathrm{SL}_2(\mathbb{F}_\ell) \sqcup \begin{bmatrix} \sqrt{\varepsilon} & 0 \\ 0 & 1/\sqrt{\varepsilon} \end{bmatrix} \mathrm{SL}_2(\mathbb{F}_\ell) \subset \mathrm{SL}_2(\mathbb{F}_{\ell^2})$$

  where ε *denotes a generator of* $\mathbb{F}_\ell^*$*, and which* $i \geqslant 2$ *corresponds the image of the cohomology class of* $2_-\mathrm{PGL}_2(\mathbb{F}_\ell)$ *by the map*

$$H^2\big(\mathrm{PGL}_2(\mathbb{F}_\ell), \mathbb{Z}/2\mathbb{Z}\big) \longrightarrow H^2\big(\mathrm{PGL}_2(\mathbb{F}_\ell), \mathbb{Z}/2^i\mathbb{Z}\big)$$

  induced by the embedding of $\mathbb{Z}/2\mathbb{Z}$ *into* $\mathbb{Z}/2^i\mathbb{Z}$*,*

- *and the group* $2^i_+\mathrm{PGL}_2(\mathbb{F}_\ell)$*, whose associated cohomology class* β_+ *is the sum in* $H^2\big(\mathrm{PGL}_2(\mathbb{F}_\ell), \mathbb{Z}/2^i\mathbb{Z}\big)$ *of* $\beta_{\det}$ *and of* β_-*.*

(iii) Let $g \in \mathrm{PGL}_2(\mathbb{F}_\ell)$ *be an element of order* 2*, and let* β_0*,* $\beta_{\det}$*,* β_- *and* β_+ *be normalised cocycles (that is to say* $\beta(1, h) = \beta(h, 1) = 0$ *for all* $h \in \mathrm{PGL}_2(\mathbb{F}_\ell)$*) representing the cohomology classes of these four extensions. If* $i = 1$*, then their value at* (g, g) *does not depend on the choice of these cocycles, and are*

- $\beta_0(g, g) = 0 \ \forall g$,
- $\beta_{\det}(g, g) = \begin{cases} 0, & g \in \mathrm{PSL}_2(\mathbb{F}_\ell), \\ 1, & g \notin \mathrm{PSL}_2(\mathbb{F}_\ell), \end{cases}$
- $\beta_-(g, g) = 1 \ \forall g$,
- $\beta_+(g, g) = \begin{cases} 1, & g \in \mathrm{PSL}_2(\mathbb{F}_\ell), \\ 0, & g \notin \mathrm{PSL}_2(\mathbb{F}_\ell). \end{cases}$

(iv) For $i \geqslant 2$*, the abelianisations of these extensions are*

- $\big(\mathbb{Z}/2^i\mathbb{Z} \times \mathrm{PGL}_2(\mathbb{F}_\ell)\big)^{\mathrm{ab}} \simeq \mathbb{Z}/2^i\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$*,*
- $\big(2^i_{\det}\mathrm{PGL}_2(\mathbb{F}_\ell)\big)^{\mathrm{ab}} \simeq \mathbb{Z}/2^{i+1}\mathbb{Z}$*,*
- $\big(2^i_-\mathrm{PGL}_2(\mathbb{F}_\ell)\big)^{\mathrm{ab}} \simeq \mathbb{Z}/2^{i-1}\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$*,*
- $\big(2^i_+\mathrm{PGL}_2(\mathbb{F}_\ell)\big)^{\mathrm{ab}} \simeq \mathbb{Z}/2^i\mathbb{Z}$*.*

Proof. We shall only give the idea of the proof here, and refer the reader to [Que95, proposition 2.4 and lemma 3.2].

(i) On the one hand, the abelianised of $\mathrm{PGL}_2(\mathbb{F}_\ell)$ is $\mathrm{PGL}_2(\mathbb{F}_\ell)/\mathrm{PSL}_2(\mathbb{F}_\ell) \simeq \mathbb{Z}/2\mathbb{Z}$, so that

$$\mathrm{Ext}^1_{\mathbb{Z}}(\mathrm{PGL}_2(\mathbb{F}_\ell)^{\mathrm{ab}}, \mathbb{Z}/2^i\mathbb{Z}) \simeq \mathrm{Ext}^1_{\mathbb{Z}}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2^i\mathbb{Z}) \simeq \mathbb{Z}/2\mathbb{Z}.$$

On the other hand, the Schur multiplier $H^2\big(\mathrm{PGL}_2(\mathbb{F}_\ell), \mathbb{C}^*\big)$ is isomorphic to $\mathbb{Z}/2\mathbb{Z}$ (cf. [Que95, proposition 2.3]). The result then follows from the split exact sequence $(\star)$.

(ii) Consider again the exact sequence $(\star)$. Then $\beta_{\det}$ lies in the image of ϕ since it is inflated from $\mathrm{PGL}_2(\mathbb{F}_\ell)^{\mathrm{ab}}$. On the other hand, for $i = 1$, β_- does not lie in $\mathrm{Im}\,\phi$, for if it did, then the associated transgression map would be trivial, so that the commutator subgroup of $2_-\mathrm{PGL}_2(\mathbb{F}_\ell)$ would meet the kernel $\pm\left[\begin{smallmatrix}1 & 0\\ 0 & 1\end{smallmatrix}\right]$ of the extension trivially, which is clearly not the case since $\left[\begin{smallmatrix}-1 & 0\\ 0 & -1\end{smallmatrix}\right]$ is a commutator in $\mathrm{SL}_2(\mathbb{F}_\ell) \subset 2_-\mathrm{PGL}_2(\mathbb{F}_\ell)$. For $i \geqslant 2$, the commutative diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathbb{Z}/2\mathbb{Z} & \longrightarrow & 2_-\mathrm{PGL}_2(\mathbb{F}_\ell) & \longrightarrow & \mathrm{PGL}_2(\mathbb{F}_\ell) & \longrightarrow & 1\\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathbb{Z}/2^i\mathbb{Z} & \longrightarrow & 2^i_-\mathrm{PGL}_2(\mathbb{F}_\ell) & \longrightarrow & \mathrm{PGL}_2(\mathbb{F}_\ell) & \longrightarrow & 1
\end{array}$$

shows that $\mathbb{Z}/2^i\mathbb{Z}$ still intersects the commutator subgroup of $2^i_-\mathrm{PGL}_2(\mathbb{F}_\ell)$ non-trivially, so that β_- does not lie in $\mathrm{Im}\,\phi$ either. The extensions $2^i_{\det}\mathrm{PGL}_2(\mathbb{F}_\ell)$ and $2^i_-\mathrm{PGL}_2(\mathbb{F}_\ell)$ thus represent different non-trivial cohomology classes in $H^2\big(\mathrm{PGL}_2(\mathbb{F}_\ell), \mathbb{Z}/2^i\mathbb{Z}\big) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, hence the result.

(iii) It is a general fact (cf. [Que95, lemma 3.1] that the image at (g, g) of a normalised cocycle representing an extension of a group G by $\mathbb{Z}/2\mathbb{Z}$ only depends on the cohomology class of this cocycle in $H^2(G, \mathbb{Z}/2\mathbb{Z})$.

- The case of the trivial extension is obvious since the zero cohomology class is represented by the zero cocycle.
- The case of $\beta_{\det}$ follows from its very definition.
- Since it is a subgroup of $\mathrm{SL}_2(\mathbb{F}_{\ell^2})$, the group $2_-\mathrm{PGL}_2(\mathbb{F}_\ell)$ has only one element of order 2, namely the central element $\left[\begin{smallmatrix}-1 & 0\\ 0 & -1\end{smallmatrix}\right]$. In particular, no element $g \in \mathrm{PGL}_2(\mathbb{F}_\ell)$ of order 2 remains of order 2 when lifted to $2_-\mathrm{PGL}_2(\mathbb{F}_\ell)$, and the result follows from lemma 3.
- The case of β_+ follows since we may take $\beta_+ = \beta_{\det} + \beta_-$.

(iv) Again, the case of the trivial extension is clear. In the other cases, the result follows from the fact that the intersection of $\mathbb{Z}/2^i\mathbb{Z}$ with the commutator subgroup of the extension is isomorphic to the image of transgression map

$$\mathrm{Tra}_\beta \colon \widehat{\mathbb{Z}/2^i\mathbb{Z}} \longrightarrow H^2\big(\mathrm{PGL}_2(\mathbb{F}_\ell), \mathbb{C}^*\big) \simeq \mathbb{Z}/2\mathbb{Z},$$

which is trivial in the case of $\beta_{\det}$ and non-trivial in the case of β_- and β_+. □

We shall now prove that $\mathrm{Gal}(L_r/\mathbb{Q})$ is isomorphic to $\mathrm{GL}_2(\mathbb{F}_\ell)/S_r$. We first deal with the first extension L_1/L_0 in the quadratic tower $L_r/\cdots/L_0$. The Galois group $\mathrm{Gal}(L_1/\mathbb{Q})$ is a (necessarily central) extension of $\mathrm{Gal}(L_0/\mathbb{Q})$, which is isomorphic by $\rho_{f,\mathfrak{l}}^{\mathrm{proj}}$ to $\mathrm{PGL}_2(\mathbb{F}_\ell)$ since L_0 is the number field cut out by $\rho_{f,\mathfrak{l}}$. Let β be a normalised cocycle representing the cohomology class corresponding to this extension. According to theorem 4(ii), $\mathrm{Gal}(L_1/\mathbb{Q})$ is isomorphic either to $\mathbb{Z}/2\mathbb{Z}\times\mathrm{PGL}_2(\mathbb{F}_\ell)$, $2_{\mathrm{det}}\mathrm{PGL}_2(\mathbb{F}_\ell)$, $2_-\mathrm{PGL}_2(\mathbb{F}_\ell)$ or $2_+\mathrm{PGL}_2(\mathbb{F}_\ell)$, and β is correspondingly cohomologous to β_0, β_{det}, β_- or β_+.

If $\mathrm{Gal}(L_1/\mathbb{Q})$ were the trivial extension $\mathbb{Z}/2\mathbb{Z}\times\mathrm{PGL}_2(\mathbb{F}_\ell)$, then L_1 would have a subextension L_1^{ab} with Galois group isomorphic to

$$\big(\mathbb{Z}/2\mathbb{Z}\times\mathrm{PGL}_2(\mathbb{F}_\ell)\big)^{\mathrm{ab}}\simeq\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z},$$

and hence three distinct quadratic subfields, which is impossible since L_1 is ramified only at ℓ by (A1).

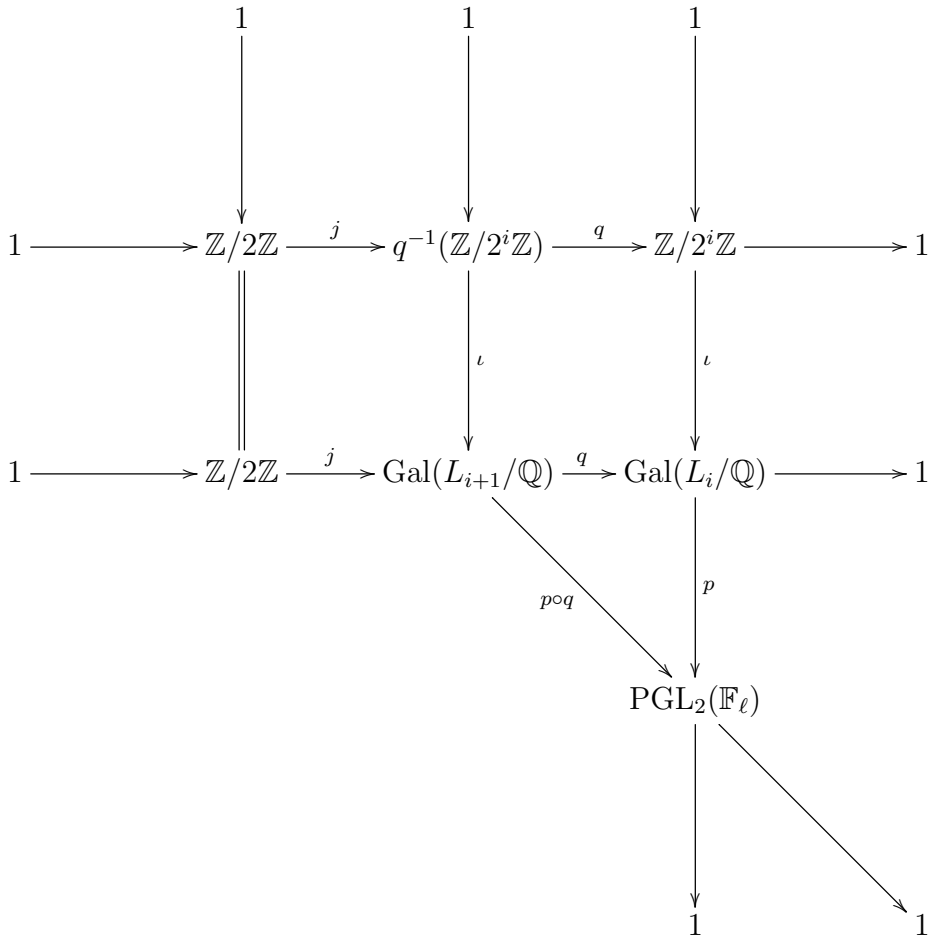
Let now $\tau_1\in\mathrm{Gal}(L_1/\mathbb{Q})$ be the complex conjugation relative to some embedding of L_1 into $\mathbb{C}$. It induces an element $\tau_0\in\mathrm{Gal}(L_0/\mathbb{Q})$, which is not the identity since its image by $\rho_{f,\mathfrak{l}}^{\mathrm{proj}}$ is conjugate to $g=\left[\begin{smallmatrix}1&0\\0&-1\end{smallmatrix}\right]\in\mathrm{PGL}_2(\mathbb{F}_\ell)$. In particular, τ_1 is not trivial either, so it has order 2. Therefore τ_0 has a lift to $\mathrm{Gal}(L_1/\mathbb{Q})$ of order 2, so that $\beta(\tau_0,\tau_0)=0$ by lemma 3. Theorem 4(iii) then only leaves one possibility: if $\ell\equiv 1 \bmod 4$, then $g\in\mathrm{PSL}_2(\mathbb{F}_\ell)$, so that β cannot be cohomologous to β_- nor to β_+ and so $\mathrm{Gal}(L_1/\mathbb{Q})$ must be isomorphic to $2_{\mathrm{det}}\mathrm{PGL}_2(\mathbb{F}_\ell)$, whereas if $\ell\equiv -1 \bmod 4$, then $g\notin\mathrm{PSL}_2(\mathbb{F}_\ell)$, so that β cannot be cohomologous to β_- nor to β_{det} and so $\mathrm{Gal}(L_1/\mathbb{Q})$ must be isomorphic to $2_+\mathrm{PGL}_2(\mathbb{F}_\ell)$.

Now let L_1' be the number field cut out by $\rho_{f,\mathfrak{l}}^{S_1}$, which is supposed to be isomorphic to L_1. Then L_1' is also a quadratic extension of L_0 and is also ramified only at ℓ, so that the same reasoning applies and shows that $\mathrm{Gal}(L_1'/\mathbb{Q})$ is isomorphic to $2_{\mathrm{det}}\mathrm{PGL}_2(\mathbb{F}_\ell)$ if $\ell\equiv 1 \bmod 4$ and to $2_+\mathrm{PGL}_2(\mathbb{F}_\ell)$ if $\ell\equiv 1 \bmod 4$. On the other hand, it is isomorphic to $\mathrm{Im}\,\rho_{f,\mathfrak{l}}^{S_1}\simeq\mathrm{GL}_2(\mathbb{F}_\ell)/S_1$ since the determinant of $\rho_{f,\mathfrak{l}}$ is an odd power of the mod ℓ cyclotomic character, so that in each case

$$\mathrm{Gal}(L_1/\mathbb{Q})\simeq\mathrm{Gal}(L_1'/\mathbb{Q})\simeq\mathrm{GL}_2(\mathbb{F}_\ell)/S_1.$$

If $\ell\equiv -1 \bmod 4$, then $r=1$, so that the proof that $\mathrm{Gal}(L_r/\mathbb{Q})\simeq\mathrm{GL}_2(\mathbb{F}_\ell)/S_r$ is over. We shall therefore concentrate on the case $\ell\equiv 1 \bmod 4$ from now on. We shall first prove by induction on i that $\mathrm{Gal}(L_i/\mathbb{Q})$ is an extension of $\mathrm{PGL}_2(\mathbb{F}_\ell)$ by $\mathbb{F}_\ell^*/S_i\simeq\mathbb{Z}/2^i\mathbb{Z}$, then that this extension is central, and finally that it is the expected one. Note that we have just proved above that it is so for $i=1$.

Let $1 \leqslant i < r$. By induction hypothesis, there is a commutative diagram



whose middle row and right column are exact. A diagram chase then reveals that the top row and the diagonal short sequence

$$1 \longrightarrow q^{-1}(\mathbb{Z}/2^i\mathbb{Z}) \xrightarrow{\iota} \mathrm{Gal}(L_{i+1}/\mathbb{Q}) \xrightarrow{p\circ q} \mathrm{PGL}_2(\mathbb{F}_\ell) \longrightarrow 1$$

are exact, so that $\mathrm{Gal}(L_{i+1}/\mathbb{Q})$ is an extension of $\mathrm{PGL}_2(\mathbb{F}_\ell)$ by $q^{-1}(\mathbb{Z}/2^i\mathbb{Z})$, which itself is an extension of $\mathbb{Z}/2^i\mathbb{Z}$ by $\mathbb{Z}/2\mathbb{Z}$, which is necessarily central since $\mathrm{Aut}(\mathbb{Z}/2\mathbb{Z})$ is trivial.

Now $H^2(\mathbb{Z}/2^i\mathbb{Z}, \mathbb{C}^*) = \{0\}$ since $\mathbb{Z}/2^i\mathbb{Z}$ is cyclic, so the extensions of of $\mathbb{Z}/2^i\mathbb{Z}$ by $\mathbb{Z}/2\mathbb{Z}$ are all abelian by the exact sequence $(\star)$, so that $q^{-1}(\mathbb{Z}/2^i\mathbb{Z}) = \mathrm{Gal}(L_{i+1}/L_0)$ is isomorphic either to $\mathbb{Z}/2^{i+1}\mathbb{Z}$ or to $\mathbb{Z}/2^i\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. We shall now prove that the latter is impossible.

Since $\ell \equiv 1 \bmod 4$, $S_1^2 = \mathbb{F}_\ell^{*4}$ is a strict subgroup of $S_1 = \mathbb{F}_\ell^{*2}$. The determinant induces a surjective morphism

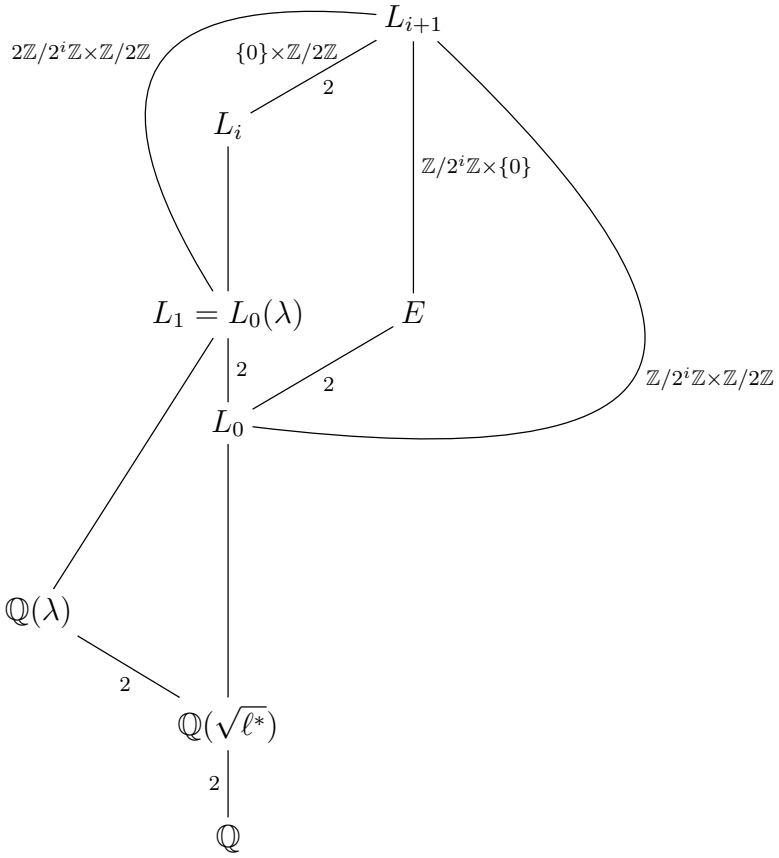
$$\mathrm{Gal}(L_1/\mathbb{Q}) \xrightarrow[\sim]{\rho_{f,\mathfrak{l}}^{S_1}} \mathrm{GL}_2(\mathbb{F}_\ell)/S_1 \xrightarrow{\det} \mathbb{F}_\ell^*/S_1^2 = \mathbb{F}_\ell^*/\mathbb{F}_\ell^{*4} \simeq \mathbb{Z}/4\mathbb{Z},$$

so that L_1 has a quartic subfield. This subfield is abelian, and it ramifies only at ℓ by (A1), so it is a subfield of $\mathbb{Q}(\mu_{\ell^\infty})$. Since

$$\mathrm{Gal}\left(\mathbb{Q}(\mu_{\ell^\infty})/\mathbb{Q}\right) \simeq \mathbb{Z}_\ell^* = \mathbb{F}_\ell^* \times (1 + \ell\mathbb{Z}_\ell) \simeq \mathbb{Z}/(\ell-1)\mathbb{Z} \times \mathbb{Z}_\ell$$

has only one quotient isomorphic to $\mathbb{Z}/4\mathbb{Z}$ (which does exist since $\ell \equiv 1 \bmod 4$), this quartic subfield is unique, and I shall denote a primitive element of it by λ. This

λ thus lies in L_1, but it cannot lie in L_0 since the maximal abelian subextension of L_0 has Galois group $\mathrm{PGL}_2(\mathbb{F}_\ell)^{\mathrm{ab}} \simeq \mathbb{Z}/2\mathbb{Z}$ (and hence is $\mathbb{Q}(\sqrt{\ell^*})$). Since $\mathbb{Q}(\lambda)$ is a quadratic extension of $\mathbb{Q}(\sqrt{\ell^*}) \subset L_0$ and L_1 is a quadratic extension of L_0, we have $L_1 = L_0(\lambda)$. Now if $\mathrm{Gal}(L_{i+1}/L_0)$ were isomorphic to $\mathbb{Z}/2^i\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, then, letting E be the subfield of L_{i+1} fixed by $\mathbb{Z}/2^i\mathbb{Z} \times \{0\}$, we would have the extension tower



The extensions E/L_0 and L_1/L_0 are both quadratic subextensions of L_{i+1}/L_0, but they are distinct since they correspond respectively to the distinct subgroups $\mathbb{Z}/2^i\mathbb{Z}\times\{0\}$ and $2\mathbb{Z}/2^i\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ of $\mathrm{Gal}(L_{i+1}/L_0) = \mathbb{Z}/2^i\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. On the other hand, the field E is a quadratic extension of L_0 which is ramified only at ℓ since L_{i+1} is by (A1), so the same reasoning as above shows that its Galois group is $\mathrm{Gal}(E/\mathbb{Q}) \simeq 2_{\mathrm{det}}\mathrm{PGL}_2(\mathbb{F}_\ell) \simeq \mathrm{GL}_2(\mathbb{F}_\ell)/S_1$ since $\ell \equiv 1 \bmod 4$, so that it has a quartic subfield, which can only be $\mathbb{Q}(\lambda)$. But then $E \supseteq L_0(\lambda) = L_1$, hence $E = L_1$ since they are both quadratic extensions of L_0, a contradiction. This shows that $\mathrm{Gal}(L_{i+1}/L_0)$ cannot be isomorphic to $\mathbb{Z}/2^i\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$, so must be isomorphic to $\mathbb{Z}/2^{i+1}\mathbb{Z}$. It follows that $\mathrm{Gal}(L_{i+1}/\mathbb{Q})$ is an extension of $\mathrm{Gal}(L_0/\mathbb{Q}) \simeq \mathrm{PGL}_2(\mathbb{F}_\ell)$ by $\mathrm{Gal}(L_{i+1}/L_0) \simeq \mathbb{Z}/2^{i+1}\mathbb{Z}$, and the induction is complete.

We shall now prove by induction on i that this extension is central. Note that it is so for $i = 1$ since $\mathrm{Aut}(\mathbb{Z}/2\mathbb{Z})$ is trivial. Let $i \geqslant 2$, and assume on the contrary that the extension

$$0 \longrightarrow \mathbb{Z}/2^i\mathbb{Z} \longrightarrow \mathrm{Gal}(L_i/\mathbb{Q}) \longrightarrow \mathrm{PGL}_2(\mathbb{F}_\ell) \longrightarrow 1$$

is not central. Since $\mathrm{Aut}(\mathbb{Z}/2^i\mathbb{Z}) \simeq (\mathbb{Z}/2^i\mathbb{Z})^*$ is abelian, the morphism $\mathrm{PGL}_2(\mathbb{F}_\ell) \longrightarrow \mathrm{Aut}(\mathbb{Z}/2^i\mathbb{Z})$ expressing the conjugation action of $\mathrm{PGL}_2(\mathbb{F}_\ell)$ on $\mathbb{Z}/2^i\mathbb{Z}$ factors through $\mathrm{PGL}_2(\mathbb{F}_\ell)^{\mathrm{ab}} = \mathrm{PGL}_2(\mathbb{F}_\ell)/\,\mathrm{PSL}_2(\mathbb{F}_\ell) \simeq \mathbb{Z}/2\mathbb{Z}$, so that $\mathrm{PSL}_2(\mathbb{F}_\ell)$ acts trivially whereas

there exists an involution ϕ of $\mathbb{Z}/2^i\mathbb{Z}$ such that $g \cdot x = \phi(x)$ for all $g \notin \mathrm{PSL}_2(\mathbb{F}_\ell)$ and $x \in \mathbb{Z}/2^i\mathbb{Z}$. By induction hypothesis, this involution induces the identity on $\mathbb{Z}/2^{i-1}\mathbb{Z}$, so it must be $x \mapsto (1+2^{i-1})x$.

There is thus only one possible non-trivial action of $\mathrm{PGL}_2(\mathbb{F}_\ell)$. In order to compute $H^2\big(\mathrm{PGL}_2(\mathbb{F}_\ell), \mathbb{Z}/2^i\mathbb{Z}\big)$ for this non-trivial action, we use the inflation-restriction exact sequence

$$0 \longrightarrow H^2(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2^i\mathbb{Z}) \xrightarrow{\mathrm{Inf}} H^2\big(\mathrm{PGL}_2(\mathbb{F}_\ell), \mathbb{Z}/2^i\mathbb{Z}\big) \xrightarrow{\mathrm{Res}} H^2\big(\mathrm{PSL}_2(\mathbb{F}_\ell), \mathbb{Z}/2^i\mathbb{Z}\big). \tag{$\dagger$}$$

This is legitimate since, as $\mathrm{PSL}_2(\mathbb{F}_\ell)$ acts trivially, we have

$$H^1\big(\mathrm{PSL}_2(\mathbb{F}_\ell), \mathbb{Z}/2^i\mathbb{Z}\big) = \mathrm{Hom}\big(\mathrm{PSL}_2(\mathbb{F}_\ell), \mathbb{Z}/2^i\mathbb{Z}\big) = 0$$

since $\mathrm{PSL}_2(\mathbb{F}_\ell)$ is simple.

On the one hand, since $\mathbb{Z}/2\mathbb{Z} = \{1, \varepsilon\}$ is cyclic, the groups $H^q(\mathbb{Z}/2\mathbb{Z}, M)$ are the cohomology groups of the complex

$$0 \longrightarrow M \xrightarrow{\varepsilon-1} M \xrightarrow{\varepsilon+1} M \xrightarrow{\varepsilon-1} M \xrightarrow{\varepsilon+1} \cdots$$

for any $\mathbb{Z}/2\mathbb{Z}$-module M (cf. [Lan02, chapter XX exercise 16]). In particular,

$$H^2(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2^i\mathbb{Z}) = \frac{\ker(\varepsilon-1)}{\mathrm{Im}(\varepsilon+1)} = \frac{(\mathbb{Z}/2^i\mathbb{Z})[2^{i-1}]}{(2+2^{i-1})(\mathbb{Z}/2^i\mathbb{Z})} \simeq \begin{cases} \mathbb{Z}/2\mathbb{Z}, & i = 2, \\ 0, & i \geqslant 3. \end{cases}$$

On the other hand, as $\mathrm{PSL}_2(\mathbb{F}_\ell)$ acts trivially, the group $H^2\big(\mathrm{PSL}_2(\mathbb{F}_\ell), \mathbb{Z}/2^i\mathbb{Z}\big)$ can be computed by using the split exact sequence $(\star)$. As $\mathrm{PSL}_2(\mathbb{F}_\ell)^{\mathrm{ab}} = \{1\}$ since $\mathrm{PSL}_2(\mathbb{F}_\ell)$ is simple, and as the Schur multiplier is

$$H^2\big(\mathrm{PSL}_2(\mathbb{F}_\ell), \mathbb{C}^*\big) \simeq \mathbb{Z}/2\mathbb{Z}$$

(Steinberg, cf. [Kar87, theorem 7.1.1.(ii)]), it results that

$$H^2\big(\mathrm{PSL}_2(\mathbb{F}_\ell), \mathbb{Z}/2^i\mathbb{Z}\big) \simeq \mathbb{Z}/2\mathbb{Z}.$$

Let $2^i\mathrm{PSL}_2(\mathbb{F}_\ell)$ denote the non-trivial extension. One has

$$2\mathrm{PSL}_2(\mathbb{F}_\ell) \simeq \mathrm{SL}_2(\mathbb{F}_\ell),$$

and the non-trivial element of $H^2\big(\mathrm{PSL}_2(\mathbb{F}_\ell), \mathbb{Z}/2^i\mathbb{Z}\big)$ is the image of the non-trivial element $\gamma_{\mathrm{SL}_2} \in H^2\big(\mathrm{PSL}_2(\mathbb{F}_\ell), \mathbb{Z}/2\mathbb{Z}\big)$ corresponding to $\mathrm{SL}_2(\mathbb{F}_\ell)$ by the map

$$H^2\big(\mathrm{PSL}_2(\mathbb{F}_\ell), \mathbb{Z}/2\mathbb{Z}\big) \longrightarrow H^2\big(\mathrm{PSL}_2(\mathbb{F}_\ell), \mathbb{Z}/2^i\mathbb{Z}\big)$$

induced by the embedding of $\mathbb{Z}/2\mathbb{Z}$ into $\mathbb{Z}/2^i\mathbb{Z}$.

Consider the inflation-restriction exact sequence $(\dagger)$, and let

$$\beta \in H^2\big(\mathrm{PGL}_2(\mathbb{F}_\ell), \mathbb{Z}/2^i\mathbb{Z}\big)$$

be the cohomology class corresponding to the extension

$$0 \longrightarrow \mathbb{Z}/2^i\mathbb{Z} \longrightarrow \mathrm{Gal}(L_i/\mathbb{Q}) \longrightarrow \mathrm{PGL}_2(\mathbb{F}_\ell) \longrightarrow 1.$$

If $\gamma = \mathrm{Res}\,\beta \in H^2\big(\mathrm{PSL}_2(\mathbb{F}_\ell), \mathbb{Z}/2^i\mathbb{Z}\big)$ were trivial, then $\beta = \mathrm{Inf}\,\alpha$ would be the inflation of some $\alpha \in H^2\big(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2^i\mathbb{Z}\big)$, so that $\mathrm{Gal}(L_i/\mathbb{Q})$ would be isomorphic

to the fibred product (a.k.a. pullback) $G_\alpha \underset{\mathbb{Z}/2\mathbb{Z}}{\times} \mathrm{PGL}_2(\mathbb{F}_\ell)$, where G_α is the group extension

$$0 \longrightarrow \mathbb{Z}/2^i\mathbb{Z} \longrightarrow G_\alpha \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 0$$

corresponding to α. Actually, if $i \geqslant 3$, then $\beta = \operatorname{Inf}\alpha$ would be trivial since $H^2\big(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2^i\mathbb{Z}\big) = 0$, so that $\mathrm{Gal}(L_i/\mathbb{Q})$ would be isomorphic to the semi-direct product

$$\mathbb{Z}/2^i\mathbb{Z} \rtimes \mathrm{PGL}_2(\mathbb{F}_\ell),$$

whereas if $i = 2$, then $H^2\big(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2^i\mathbb{Z}\big) \simeq \mathbb{Z}/2\mathbb{Z}$, so that $\mathrm{Gal}(L_2/\mathbb{Q})$ would be isomorphic either to $\mathbb{Z}/4\mathbb{Z} \rtimes \mathrm{PGL}_2(\mathbb{F}_\ell)$ or to $Q_8 \underset{\mathbb{Z}/2\mathbb{Z}}{\times} \mathrm{PGL}_2(\mathbb{F}_\ell)$, where Q_8, the quaternionic group $\{\pm 1, \pm i, \pm j, \pm k\}$, is the extension

$$0 \longrightarrow \mathbb{Z}/4\mathbb{Z} \longrightarrow Q_8 \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 0$$

corresponding to the non-trivial element of $H^2(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/4\mathbb{Z})$. However, since the abelianisations

$$\Big(\mathbb{Z}/2^i\mathbb{Z} \rtimes \mathrm{PGL}_2(\mathbb{F}_\ell)\Big)^{\mathrm{ab}} \simeq \mathbb{Z}/2^{i-1}\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

and

$$\big(Q_8 \underset{\mathbb{Z}/2\mathbb{Z}}{\times} \mathrm{PGL}_2(\mathbb{F}_\ell)\big)^{\mathrm{ab}} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

have 2-rank 2, this is impossible, since L_i ramifies only at ℓ by (A1) and there is only one quadratic number field which ramifies only at ℓ, namely $\mathbb{Q}(\sqrt{\ell^*})$.

It follows that $\gamma = \mathrm{Res}\,\beta \in H^2\big(\mathrm{PSL}_2(\mathbb{F}_\ell), \mathbb{Z}/2^i\mathbb{Z}\big)$ cannot be trivial, so it must be $\gamma_{\mathrm{SL}_2} \in H^2\big(\mathrm{PSL}_2(\mathbb{F}_\ell), \mathbb{Z}/2\mathbb{Z}\big)$ followed by the embedding of $\mathbb{Z}/2\mathbb{Z}$ into $\mathbb{Z}/2^i\mathbb{Z}$. Let $g = \left[\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right] \in \mathrm{PGL}_2(\mathbb{F}_\ell)$. As $\ell \equiv 1 \bmod 4$, g lies in $\mathrm{PSL}_2(\mathbb{F}_\ell)$, and since the only element of order 2 of $\mathrm{SL}_2(\mathbb{F}_\ell)$ is $\left[\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right]$, g cannot be lifted to an element of order 2 of $\mathrm{SL}_2(\mathbb{F}_\ell)$, so that $\gamma_{\mathrm{SL}_2}(g, g) \neq 0$ by lemma 3. On the other hand, since g is the image of the complex conjugation (with respect to some embedding of L_0 into $\mathbb{C}$) by the projective Galois representation $\rho_{f,\mathfrak{l}}^{\mathrm{proj}}$, it must lift to an element of order 2 of $\mathrm{Gal}(L_i/\mathbb{Q})$, which is contradictory: in the extension $\mathrm{Gal}(L_i/\mathbb{Q})$, seen as the set $\mathbb{Z}/2^i\mathbb{Z} \times \mathrm{PGL}_2(\mathbb{F}_\ell)$ endowed with the group law

$$(x_1, g_1) \cdot (x_2, g_2) = \big(x_1 + g_1 \cdot x_2 + \beta(g_1, g_2), g_1 g_2\big),$$

we compute that

$$(x, g) \cdot (x, g) = \big(x + g \cdot x + \beta(g, g), g^2\big) = \big(\beta(g, g), 1\big)$$

as $g \in \mathrm{PSL}_2(\mathbb{F}_\ell)$ acts trivially, so $\beta(g, g)$ must be zero, but $\beta(g, g) = \gamma_{\mathrm{SL}_2}(g, g) \neq 0$ since $g \in \mathrm{PSL}_2(\mathbb{F}_\ell)$.

It is therefore impossible that the extension

$$0 \longrightarrow \mathbb{Z}/2^i\mathbb{Z} \longrightarrow \mathrm{Gal}(L_i/\mathbb{Q}) \longrightarrow \mathrm{PGL}_2(\mathbb{F}_\ell) \longrightarrow 1$$

be not central, which completes the induction.

In particular, $\mathrm{Gal}(L_r/\mathbb{Q})$ is a central extension of $\mathrm{Gal}(L_0/\mathbb{Q}) \simeq \mathrm{PGL}_2(\mathbb{F}_\ell)$ by $\mathrm{Gal}(L_r/L_0) \simeq \mathbb{Z}/2^r\mathbb{Z}$, so that it is isomorphic either to $\mathbb{Z}/2^r\mathbb{Z} \times \mathrm{PGL}_2(\mathbb{F}_\ell)$, $2^r_{\mathrm{det}}\mathrm{PGL}_2(\mathbb{F}_\ell)$, $2^r_-\mathrm{PGL}_2(\mathbb{F}_\ell)$ or $2^r_+\mathrm{PGL}_2(\mathbb{F}_\ell)$ by theorem 4(ii). Let L_r^{ab} be the maximal subfield of

L_r which is abelian over $\mathbb{Q}$. Then its Galois group is the abelianised of $\mathrm{Gal}(L_r/\mathbb{Q})$, which is thus respectively isomorphic to $\mathbb{Z}/2^r\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/2^{r+1}\mathbb{Z}$, $\mathbb{Z}/2^{r-1}\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ or $\mathbb{Z}/2^r\mathbb{Z}$ by theorem 4(iv). This allows to exclude $\mathbb{Z}/2^r\mathbb{Z}\times\mathrm{PGL}_2(\mathbb{F}_\ell)$ and $2^r_-\mathrm{PGL}_2(\mathbb{F}_\ell)$ since L_r, which ramifies only at ℓ by (A1), can only have one quadratic subfield. Furthermore, since L_r^{ab} is abelian and ramifies only at ℓ, it is a subfield of $\mathbb{Q}(\mu_{\ell^\infty})$, so that its Galois group $\mathrm{Gal}(L_r/\mathbb{Q})^{\mathrm{ab}}$ is a quotient of

$$\mathrm{Gal}\left(\mathbb{Q}(\mu_{\ell^\infty})/\mathbb{Q}\right)\simeq\mathbb{Z}_\ell^*\simeq\mathbb{Z}/(\ell-1)\mathbb{Z}\times\mathbb{Z}_\ell.$$

In particular, this quotient cannot be isomorphic to $\mathbb{Z}/2^{r+1}\mathbb{Z}$ since $\ell-1=2^rs$, $s\in\mathbb{N}$ odd, so $\mathrm{Gal}(L_r/\mathbb{Q})$ cannot be isomorphic to $2^r_{\mathrm{det}}\mathrm{PGL}_2(\mathbb{F}_\ell)$ either. It must therefore be isomorphic to $2^r_+\mathrm{PGL}_2(\mathbb{F}_\ell)$. Besides, the same reasoning applies to the number field cut out by the quotient Galois representation $\rho_{f,\mathfrak{l}}^{S_r}$, whose Galois group is isomorphic to the image of $\rho_{f,\mathfrak{l}}^{S_r}$, which is the whole of $\mathrm{GL}_2(\mathbb{F}_\ell)/S_r$ since the determinant of $\rho_{f,\mathfrak{l}}$ is an odd power of the mod ℓ cyclotomic character. Therefore, $\mathrm{Gal}(L_r/\mathbb{Q})$ is isomorphic to $\mathrm{GL}_2(\mathbb{F}_\ell)/S_r$.

Remark 5. From there, we can go back down the quadratic tower $L_r/\cdots/L_0$ and see that $\mathrm{Gal}(L_i/\mathbb{Q})\simeq\mathrm{GL}_2(\mathbb{F}_\ell)/S_i$ for all i. Besides, it is easy to see that the abelianised of $\mathrm{GL}_2(\mathbb{F}_\ell)/S_i$ is $\mathbb{F}_\ell^*/S_i^2$, the projection being induced by the determinant. Since $S_i^2=S_{i+1}\subsetneq S_i$ for $i<r$ whereas $S_r^2=S_r$ as $-1\notin S_r$, theorem 4(iv) leads to the unified formula

$$\mathrm{Gal}(L_i/\mathbb{Q})\simeq\mathrm{GL}_2(\mathbb{F}_\ell)/S_i\simeq\begin{cases}\mathrm{PGL}_2(\mathbb{F}_\ell), & i=0,\\ 2^i_{\mathrm{det}}\mathrm{PGL}_2(\mathbb{F}_\ell), & 0<i<r,\\ 2^r_+\mathrm{PGL}_2(\mathbb{F}_\ell), & i=r,\end{cases}$$

which is valid for $\ell\equiv1 \bmod 4$ and for $\ell\equiv-1 \bmod 4$ as well, and which allows to identify for each i the extension $\mathrm{GL}_2(\mathbb{F}_\ell)/S_i$ of $\mathrm{PGL}_2(\mathbb{F}_\ell)$ amongst the ones listed in theorem 4(ii).

It follows that there exists a quotient Galois representation

$$\rho^{S_r}\colon G_{\mathbb{Q}}\longrightarrow\!\!\!\!\!\rightarrow\mathrm{Gal}(L_r/\mathbb{Q})\xrightarrow{\sim}\mathrm{GL}_2(\mathbb{F}_\ell)/S_r$$

which cuts out the field L_r and whose projectivisation

$$G_{\mathbb{Q}}\xrightarrow{\rho^{S_r}}\mathrm{GL}_2(\mathbb{F}_\ell)/S_r\longrightarrow\!\!\!\!\!\rightarrow\mathrm{PGL}_2(\mathbb{F}_\ell)$$

is isomorphic to $\rho_{f,\mathfrak{l}}^{\mathrm{proj}}$. This representation ρ^{S_r} is therefore a twist $\rho_{f,\mathfrak{l}}^{S_r}\otimes\psi$ of $\rho_{f,\mathfrak{l}}^{S_r}$ by a Galois character

$$\psi\colon G_{\mathbb{Q}}\longrightarrow\mathbb{F}_\ell^*/S_r.$$

The number field cut out by ψ is abelian and, since it is contained in L_r, it ramifies only at ℓ by (A1), so it is a subfield of $\mathbb{Q}(\mu_{\ell^\infty})$. Besides, its Galois group is isomorphic to the image of ψ, whose order is prime to ℓ, so that this field is a subfield of $\mathbb{Q}(\mu_\ell)$, which is also contained L_r^{ab}. Since $\mathrm{Gal}\left(\mathbb{Q}(\mu_\ell)/\mathbb{Q}\right)\simeq\mathbb{Z}/(\ell-1)\mathbb{Z}$ is cyclic and since the order of $\mathrm{Im}\,\psi\subset\mathbb{F}_\ell^*/S_r$ divides the order of $\mathrm{Gal}(L_r^{\mathrm{ab}}/\mathbb{Q})\simeq\mathbb{F}_\ell^*/S_r$, the number field cut out by ψ is contained in L_r^{ab}. The kernel of the quotient representation $\rho\sim\rho_{f,\mathfrak{l}}^{S_r}\otimes\psi$ therefore agrees with the kernel of $\rho_{f,\mathfrak{l}}^{S_r}$, which completes the proof of the fact that the decomposition field of the polynomial $F_r(X)$ computed by the algorithm is the number field cut out by $\rho_{f,\mathfrak{l}}^{S_r}$.

Remark 6. Since the linear Galois representation $\rho_{f,\mathfrak{l}}$ can be recovered from the quotient Galois representation $\rho_{f,\mathfrak{l}}^{S_r}$ and the mod ℓ cyclotomic character $\overline{\chi}_\ell$ as

$$\rho_{f,\mathfrak{l}}\colon G_{\mathbb{Q}} \xrightarrow{\rho_{f,\mathfrak{l}}^{S_r}\times\overline{\chi}_\ell^{k-1}} \mathrm{GL}_2(\mathbb{F}_\ell)/S_r \times \mathbb{F}_\ell^* \xrightarrow{\quad\phi^{-1}\quad} \mathrm{GL}_2(\mathbb{F}_\ell)$$

where

$$\begin{array}{rccc} \phi\colon & \mathrm{GL}_2(\mathbb{F}_\ell) & \longrightarrow & \mathrm{GL}_2(\mathbb{F}_\ell)/S \times \mathbb{F}_\ell^* \\ & g & \longmapsto & \big(\pi(g), \det(g)\big) \end{array}$$

(cf. [Mas13, section 3.7.2]), the number field L cut out by the linear representation $\rho_{f,\mathfrak{l}}$ is the compositum of the number field L_r cut out by $\rho_{f,\mathfrak{l}}^{S_r}$ and of the number field $E \subseteq \mathbb{Q}(\mu_\ell)$ cut out by $\overline{\chi}_\ell^{k-1}$. This yields an easy method to compute a nice monic polynomial in $\mathbb{Z}[X]$ whose decomposition field is L: using [Pari/GP], first compute a polynomial defining the subcyclotomic field E by using the `polsubcyclo` function, then apply the `polcompositum` function to $F_r(X)$ and to this polynomial.

This is useful since the polynomial $F(X)$ computed by the algorithm is usually too big to be reduced, even by the methods presented in section 2.

References

[BFSS06] Bostan, Alin; Flajolet, Philippe; Salvy, Bruno; Schost, Éric, **Fast computation of special resultants**. Journal of Symbolic Computation 41, 1 (2006), pp. 1–29.

[BS14] Belabas, Karim; Simon, Denis, **Ideal power detection over number fields**. In preparation. Personal communication.

[Bos07] Bosman, Johan, **On the computation of Galois representations associated to level one modular forms**. arXiv:0710.1237

[Coh93] Cohen, Henri, **A course in computational algebraic number theory**. Graduate Texts in Mathematics, 138. Springer-Verlag, Berlin, 1993. xii+534 pp. ISBN: 3-540-55640-0.

[CE11] **Computational aspects of modular forms and Galois representations**. Edited by Bas Edixhoven and Jean-Marc Couveignes, with contributions by Johan Bosman, Jean-Marc Couveignes, Bas Edixhoven, Robin de Jong, and Franz Merkl. Ann. of Math. Stud., 176, Princeton Univ. Press, Princeton, NJ, 2011.

[Del71] Deligne, Pierre, **Formes modulaires et représentations l-adiques**. Lecture Notes in Math. 179 (1971), pp 139–172.

[Dok10] Dokchitser, Tim and Vladimir, **Identifying Frobenius elements in Galois groups**. September 2010 preprint, to appear in Algebra and Number Theory.

[FW02] Farmer, D. W.; James, K., **The irreducibility of some level 1 Hecke polynomials**. Mathematics of Computation, Vol. 71, No. 239 (Jul., 2002), pp. 1263–1270.

[Gro90] Gross, Benedict H., **A tameness criterion for Galois representations associated to modular forms (mod p)**. Duke Math. J. 61 (1990), no. 2, 445–517.

[Kar87] Karpilovsky, Gregory, **The Schur multiplier**. London Mathematical Society Monographs. New Series, 2. The Clarendon Press, Oxford University Press, New York, 1987. x+302 pp. ISBN: 0-19-853554-6.

[KW09] Khare, Chandrashekhar; Wintenberger, Jean-Pierre, **Serre's modularity conjecture (I and II)**. Inventiones Mathematicae 178 (3), pp. 485–504 and 505–586.

[Lan02] Lang, Serge, **Algebra**. Revised third edition. Graduate Texts in Mathematics, 211. Springer-Verlag, New York, 2002. xvi+914 pp. ISBN: 0-387-95385-X.

[Mas13] Mascot, Nicolas, **Computing modular Galois representations**. Rendiconti del Circolo Matematico di Palermo, Volume 62, Number 3, December 2013, pp. 451–476.

[MT03] Moon, Hyunsuk; Taguchi, Yuichiro, **Refinement of Tates discriminant bound and non-existence theorems for mod p Galois representations**. Doc. Math. Extra Vol. (2003), 641–654.

[Pari/GP] **PARI/GP**, version 2.6.0. `http://pari.math.u-bordeaux.fr/`

[Que95] Quer, Jordi, **Liftings of projective 2-dimensional Galois representations and embedding problems**. Journal of Algebra, volume 171, issue 2, 15 January 1995, pp. 541–566.

[Rib85] Ribet, Kenneth A., **On l-adic representations attached to modular forms II**. Glasgow Math. J. 27 (1985), 185–194.

[SAGE] **SAGE mathematics software**, version 5.3. `http://sagemath.org/`

[Swi72] Swinnerton-Dyer, H. P. F., **On ℓ-adic representations and congruences for coefficients of modular forms**. Modular functions of one variable, III (Proc. Internat. Summer School, Univ. Antwerp, 1972), pp. 1–55. Lecture Notes in Math., Vol. 350, Springer, Berlin, 1973.